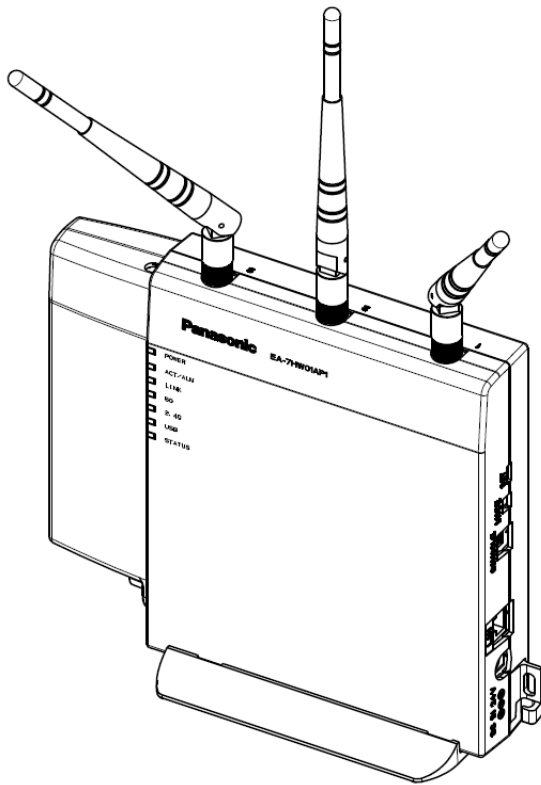
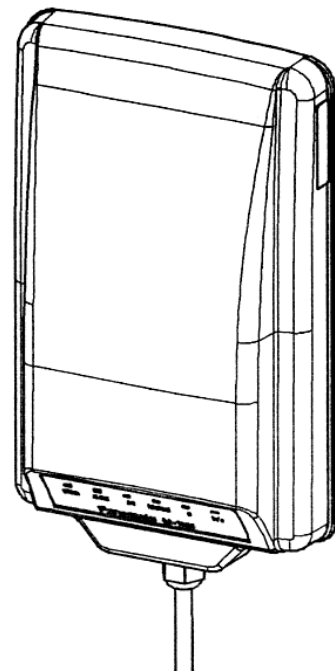
Panasonic®

取扱説明書(設定編)

屋内/屋外用無線 LAN アクセスポイント

品番 EA-7HW01AP1

品番 EA-7HW01AP2

屋内用無線 LAN アクセスポイント
EA-7HW01AP1

屋外用無線 LAN アクセスポイント
EA-7HW01AP2

このたびは、パナソニック製品をお買い上げいただき、誠にありがとうございます。

■取扱説明書(設定編)をよくお読みのうえ、正しく安全にお使いください。
ご使用の前に「**安全上のご注意**」(8～10 ページ)**を必ずお読みください。**
この取扱説明書(設定編)は大切に保管してください。

はじめに

この取扱説明書(設定編)は、屋内用無線 LAN アクセスポイント（EA-7HW01AP1）および屋外用無線 LAN アクセスポイント（EA-7HW01AP2）を利用される方が、正しく、安全に運用保守を行えることを目的として書かれています。各装置を取り扱う前にこの取扱説明書(設定編)をよく読み、書かれている指示や注意を十分に理解してください。また、この取扱説明書(設定編)は必要な時にすぐ参照できるよう使いやすい場所に保管してください。
無線 LAN アクセスポイントの設置については、別紙「取扱説明書(設計・工事編)」をお読みください。

＜商標について＞
・ イーサネット/Ethernet は、富士ゼロックス株式会社の登録商標です。
・ Microsoft とそのロゴ、Windows とそのロゴは米国 Microsoft Corporation の米国およびその他の国における登録商標です。
・ その他、本文中に記載の各会社名、各製品名は、各社の商標または、登録商標です。

＜ご使用にあたっての注意＞
パナソニック システムネットワークス株式会社は、それぞれ本書に記述されている製品および技術に関する知的所有権を所有または管理しています。これらの製品、技術、および本書は、著作権法、特許権などの知的所有権に関する法律および国際条約により保護されています。

本書およびそれに付属する製品および技術は、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。パナソニック システムネットワークス株式会社およびそのライセンサーの書面による事前の許可なく、このような製品または技術および本書のいかなる部分も、いかなる方法によっても複製することが禁じられます。本書の提供は、明示的であるか黙示的であるかを問わず、本製品またはそれに付随する技術に関するいかなる権利またはライセンスを付与するものでもありません。本書は、パナソニック システムネットワークス株式会社の一部、あるいはそのいずれかの関連会社のいかなる種類の義務を含むものでも示すものでもありません。

本書および本書に記述されている製品および技術には、ソフトウェアおよびフォント技術を含む第三者の知的財産が含まれている場合があります。これらの知的財産は、著作権法により保護されているか、または提供者からパナソニック システムネットワークス株式会社へライセンスが付与されているか、あるいはその両方です。

免責条項: 本書または本書に記述されている製品や技術に関してパナソニック システムネットワークス株式会社またはそのいずれかの関連会社が行う保証は、製品または技術の提供に適用されるライセンス契約で明示的に規定されている保証に限ります。このような契約で明示的に規定された保証を除き、パナソニック システムネットワークス株式会社およびそのいずれかの関連会社は、製品、技術、または本書に関して、明示、黙示を問わず、いかなる種類の保証も行いません。これらの製品、技術、または本書は、現状のまま提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も、かかる免責が法的に無効とされた場合を除き、行われないものとします。このような契約で明示的に規定されていないかぎり、パナソニック システムネットワーク

ス株式会社またはそのいずれかの関連会社は、いかなる法理論のもとの第三者に対しても、その収益の損失、有用性またはデータに関する損失、あるいは業務の中断について、あるいは間接的損害、特別損害、付随的損害、または結果的損害について、そのような損害の可能性が示唆されていた場合であっても、適用される法律が許容する範囲内で、いかなる責任も負いません。

本書は、「現状のまま」提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も、かかる免責が法的に無効とされた場合を除き、行われないものとします。

<お知らせ>

・ Microsoft Corporation のガイドラインに従って画面写真を使用しています。

・ この取扱説明書(設定編)の内容については、改良のため、予告なく変更する場合があります。

・ この取扱説明書(設定編)の中で特にことわり書きが無い場合は、「本装置」、「無線 LAN アクセスポイント」、「AP」、「無線ユニット」は、屋内用無線 LAN アクセスポイント（EA-7HW01AP1）および屋外用無線 LAN アクセスポイント（EA-7HW01AP2）のことを示しています。

<OSS（Open Source Software）ライセンス>

本装置のソフトウェアは、下記のオープンソースソフトウェアライセンスを使用しています。

無線 LAN アクセスポイントについて

- 本装置の故障、誤動作、不具合、或いは停電時の外部要因によって通話、録音等の機会を逸したために生じた損害等の純粋経済損害につきましては、当社は一切の責任を負いかねますので、予め御了承ください。
- 地震、雷、風水害などの天災、火災、第三者による行為、その他の事故、お客様の故意、過失及び誤用、その他異常な条件下での使用により生じた損害、および本装置の使用または使用不能から生ずる付随的な損害について、当社は一切の責任を負いかねますので、予め御了承ください。
- 本装置は、医療機器、生命維持装置、航空交通管制機器、その他人命に関わる機器・装置・システムでの使用を意図しておりません。本装置をこれらの機器・装置・システムなどに使用され生じた損害について、当社は責任を負いかねますので、予め御了承ください。

もくじ

安全上のご注意 （必ずお守りください）

人への危害、財産の損害を防止するため、必ずお守りいただくことを説明しています。

■誤った使い方をしたときに生じる危害や損害の程度を区分して、説明しています。

警告	「死亡や重傷を負うおそれがある内容」です。
	「軽傷を負うことや、財産の損害が発生するおそれがある内容」です。

■お守りいただく内容を次の図記号で説明しています。（次は図記号の例です）

	してはいけない内容です。
	実行しなければならない内容です。

安全上のご注意 (必ずお守りください)

⚠ 警告

<table>
<tr><td>
分解禁止</td><td>■分解・改造をしない
火災・感電の原因になります。</td></tr>
<tr><td>
ぬれ手禁止</td><td>■ぬれた手で、電源プラグの抜き差しはしない
感電の原因になります。</td></tr>
<tr><td rowspan="11">
禁止</td><td>■ブレーカや配線器具の定格を超える使い方や、交流 100V 以外では使用しない
定格を超えると、発熱による火災の原因になります。</td></tr>
<tr><td>■指定の AC アダプタ、PoE インジェクタ以外は使用しない
指定以外のものを使用すると、火災・感電の原因になります。</td></tr>
<tr><td>■同梱された電源コードは他の製品に使用しない
火災・感電の原因になります。</td></tr>
<tr><td>■自動ドア、火災報知器などの自動制御機器の近くには設置しない
本製品からの電波が自動制御機器に影響を及ぼすことがあり、誤動作による事故の原因になります。</td></tr>
<tr><td>■医療機器の近くには設置しない
本装置からの電波が、医療機器に影響を及ぼすことがあり、誤動作による事故の原因になります。</td></tr>
<tr><td>■電源コード・プラグ・AC アダプタ・PoE インジェクタを破損するようなことはしない
（傷つける、加工する、熱器具に近づける、無理に曲げる、ねじる、引っ張る、重い物を載せる、束ねる　など）
感電・ショート・火災の原因になります。</td></tr>
<tr><td>■屋内用無線 LAN アクセスポイント・オプションアンテナ・AC アダプタ・PoE インジェクタを水につけたり、水をかけたり、ぬらしたりしない
ショートにより、火災や感電の原因になります。</td></tr>
<tr><td>■塩害や腐食性ガスの発生する場所に設置しない
取り付け部が劣化して、落下など事故の原因になります。</td></tr>
<tr><td>■荷重に耐えられない場所や不安定な場所には設置しない
落下など事故の原因になります。</td></tr>
<tr><td>■雷が発生したときは、アクセスポイント・オプションアンテナ・AC アダプタ・PoE インジェクタや接続ケーブル類に触れない
感電の原因になります。</td></tr>
<tr><td>■使用を終了した装置は、放置しない
そのまま放置しておくと、落下など事故の原因になります。</td></tr>
</table>

安全上のご注意 必ずお守りください

⚠ 警告

<table>
<tr><td rowspan="5">
必ず守る</td><td>■心臓ペースメーカの装着部位から 22cm 以上離す
電波によりペースメーカの作動に影響を与える場合があります。</td></tr>
<tr><td>■電源プラグは根元まで確実に差し込む
差し込みが不完全ですと、感電や発熱による火災の原因になります。
●傷んだプラグ、ゆるんだコンセントは使用しないでください。</td></tr>
<tr><td>■電源プラグのほこり等は定期的にとる
プラグにほこり等がたまると、湿気等で絶縁不良となり火災の原因になります。
●電源プラグを抜き、乾いた布でふいてください。</td></tr>
<tr><td>■煙が出たり、異常発熱したり、異臭・異音がした場合や落下・破損した場合は、電源プラグをコンセントから抜き、本装置の使用を中止する
そのまま使用すると火災や感電の原因になります。
●すぐに使用を中止し、修理依頼窓口にご相談ください。</td></tr>
<tr><td>■モルタル壁などへの取り付け時、取り付け金具、ねじ等をメタルラス、ワイヤラス又は金属板と接触しないように設置する
装置の絶縁が劣化した場合、メタルラス等に漏電し、火災の原因になります。</td></tr>
</table>

⚠ 注意

<table>
<tr><td rowspan="3">
禁止</td><td>■工事中に本装置を落下させない
けがの原因になることがあります。</td></tr>
<tr><td>■高温になる場所に設置しない
装置内部の温度が上がり、火災や感電の原因になることがあります。</td></tr>
<tr><td>■金属のエッジを手でこすらない
強くこすると、けがの原因になることがあります。</td></tr>
<tr><td rowspan="3">
必ず守る</td><td>■コンセントへの抜き差しは電源プラグを持っておこなう
電源コードを引っ張ると、コードが破損し、感電、ショートや火災の原因になることがあります。</td></tr>
<tr><td>■長時間使用しないときや、お手入れ、保守をするときは必ず電源プラグをコンセントから抜く
漏電・感電の原因になることがあります。</td></tr>
<tr><td>■取り付け設置時、指定の固定方法で取り付けをする
正しく設置を行わないと、ゆるみやはずれで落下し、事故の原因になることがあります。
●設置方法については、必ず取扱説明書(設計・工事編)をお読みください。</td></tr>
</table>

使用上のお願い

- **お手入れをするときは、電源を切った状態で行ってください。機器は、乾いた柔らかい布でふいてください。**
  汚れがひどい場合は、柔らかい布に薄めた台所用洗剤（中性）をしみこませ、固く絞ったものでふき、乾いた柔らかい布で仕上げてください。

- **お手入れにアルコール、石油、シンナー、ベンジン、熱湯、みがき粉、粉せっけん、ワックスは使わないでください。**
  化学ぞうきんをご使用のときは、その注意書きに従ってください。

- **暖房設備、ボイラーなどの、特に温度の上がる場所に置かないでください。**
  機器表面や部品が変形・劣化するほか、故障の原因になります。

- **火気を近づけないでください。**
  機器表面や部品が変形・劣化するほか、故障の原因になります。

- **硫化水素、リン、アンモニア、硫黄、炭素、酸、塵埃、その他有毒ガスなどの発生する場所に置かないでください。**
  故障や機器の寿命が短くなる原因になります。

- **電磁波発生源や磁気を帯びたもののある場所に置かないでください。（高周波ミシン・電気溶接機・磁石など）**
  雑音の発生や故障の原因になります。

- **機器に強い衝撃や振動を与えないでください。**
  落としたりぶつけたりして強い衝撃が加わると、故障や破損の原因になります。

- **廃棄時は、産業廃棄物として適切に処理してください。**

電波に関する留意点

- 本装置は、電波法に基づく無線設備（2.4GHz 帯高度化小電力データ通信システム、2.4GHz 帯小電力データ通信システムおよび 5GHz 帯小電力データ通信システム）の技術基準への適合が証明されています。したがって、本装置を使用するときに無線局の免許は必要ありません。また、本装置は日本国内のみで使用できます。

- 本装置は、技術基準の適合が証明されておりますので、以下の事項を行うと法律により罰せられることがあります。
  ■本装置を分解／改造すること（周波数帯、アンテナの変更をしてはいけない）
  ■本装置の裏面に貼ってある認証ラベルをはがすこと

- 5GHz 帯（IEEE802.11a/n）は電波法により屋外で使用可能な周波数が制限されています。
  ■5GHz 帯（IEEE802.11a/n）の対応チャネルは、36ch ～ 48ch（W52）、52ch ～ 64ch（W53）、100ch ～ 140ch（W56）です。
  ■W52 および W53 は屋内使用限定です。W56 は屋外でも使用可能です。屋外使用時には、W52 もしくは W53 を選択しないように設定を行ってください。
  ■W53 および W56 に対応するため、電波制御機能 DFS、TPC が使用されています。
  ■2005 年 5 月省令改定以前のチャネル（J52）を使用した無線 LAN 機器とは、チャネルが一致しないために通信を行うことができません。

- 2.4 GHz 帯（IEEE802.11b/g/n）の使用周波数帯では、電子レンジや産業・科学・医療機器のほか工場の製造ラインなどで使用されている移動体識別用の構内無線局（免許を要する無線局）および特定小電力無線局（免許を要しない無線局）が運用されています。
  ■本装置を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局、およびアマチュア無線局が運用されていないことを確認してください。
  ■万一、本装置から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、すみやかに本製品の使用周波数を変更して、電波干渉をしないようにしてください。
  ■その他、本装置から移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して有害な電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、ご購入になった販売窓口までご連絡ください。

  使用周波数帯域　：2.4 GHz
  変調方式　：DS-SS 方式／ OFDM 方式
  想定干渉距離　：40 m 以下
  周波数変更の可否　：全帯域を使用し、かつ「構内無線局」「特定小電力無線局」帯域を回避可能
  本装置には、これを示す右記のマークが貼付されます。

2.4 DS/OF 4

無線LAN製品ご使用時におけるセキュリティーに関するご注意

● 無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコンなどと本装置間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物（壁など）を越えてすべての場所に届くため、セキュリティーに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

■ 通信内容を盗み見られる

・悪意ある第三者が、電波を故意に傍受し、

ID やパスワード又はクレジットカード番号などの個人情報

メールの内容

などの通信内容を盗み見られる可能性があります。

■ 不正に侵入される

・悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、

個人情報や機密情報を取り出す（情報漏洩）

特定の人物になりすまして通信し、不正な情報を流す（なりすまし）

傍受した通信内容を書き換えて発信する（改ざん）

コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

などの行為をされてしまう可能性があります。

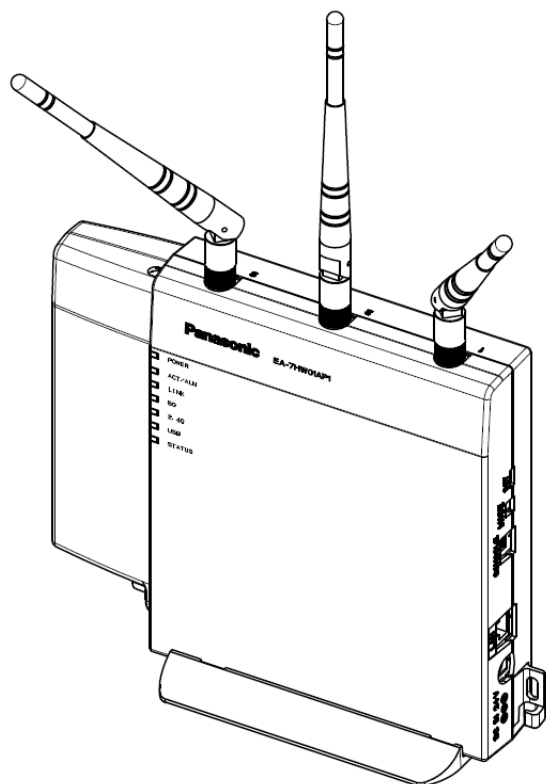
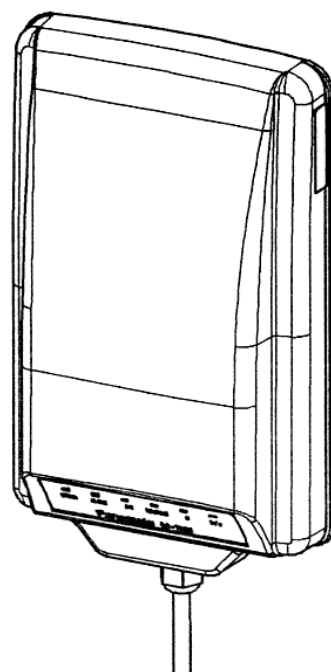
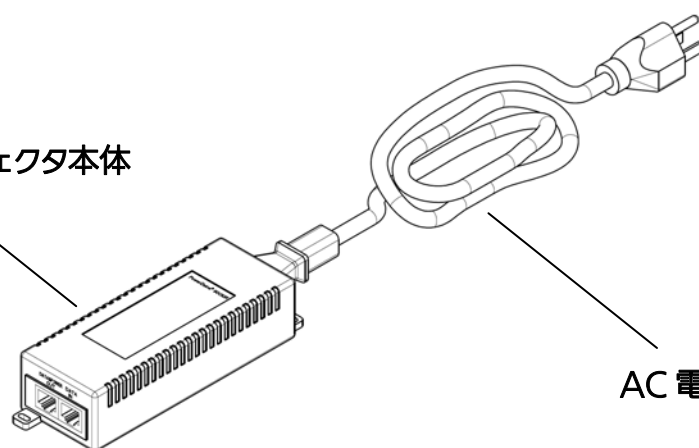
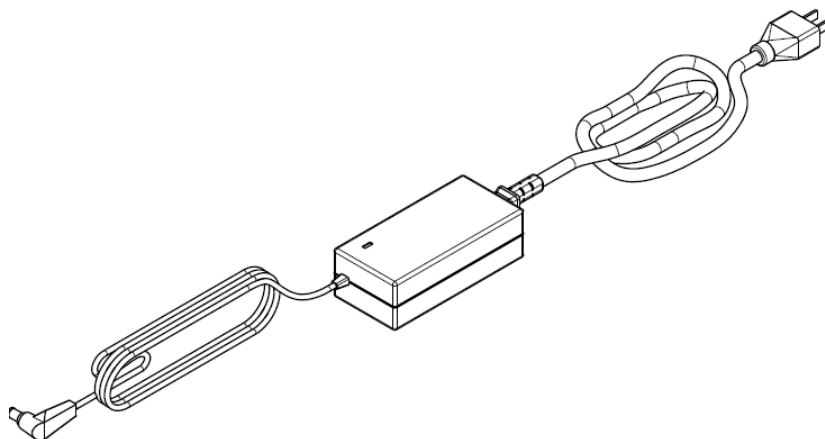
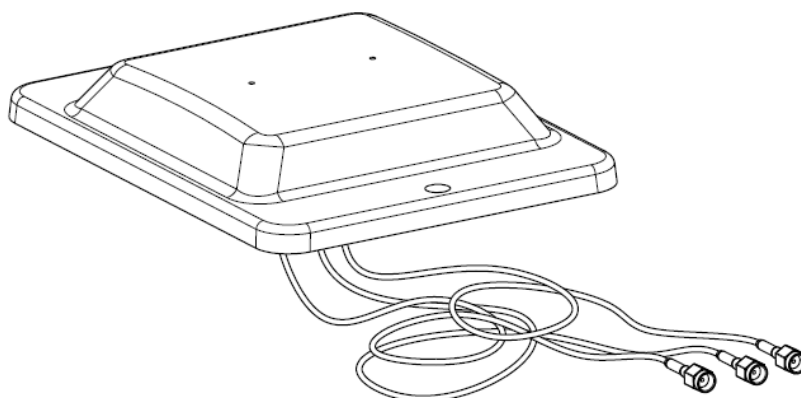
本来、無線 LAN カードや無線 LAN アクセスポイントは、これらの問題に対応するためのセキュリティーの仕組みを持っていますので、無線 LAN 製品のセキュリティーに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティーの設定を行わないで使用した場合の問題を十分理解した上で、お客様自身の判断と責任においてセキュリティーに関する設定を行い、併せてご使用になられる環境に応じたその他対応（物理的なセキュリティーによる盗難対策や VPN 機能の利用による盗聴防止など）を行った上で製品を使用することをお奨めします。

第１章　概要

本装置の製品構成および特長を紹介します。

1.1　製品構成

本装置は、無線 LAN アクセスポイント本体と PoE インジェクタで構成されます。

屋内用無線 LAN アクセスポイント
EA-7HW01AP1

屋外用無線 LAN アクセスポイント
EA-7HW01AP2

PoE インジェクタ
EA-7HW00PWR1

AC アダプタ
EA-7HW00PWR2
（屋内用無線 LAN アクセスポイントのみ）

オプションアンテナ
EA-7HW00ANT1
（屋内用無線 LAN アクセスポイントのみ）

1.2　製品の特長

1.2.1.　450Mbps の高速伝送性能

本装置では、802.11a/b/g に加えて、802.11n にも対応しています。802.11n では様々な規格が存在しますが、空間ストリーム数 3、伝送帯域幅 40MHz、ガードインターバル 400ns の 3 つの規格すべてに対応することで、5GHz 帯無線インターフェースで 450Mbps の伝送速度を実現しています。

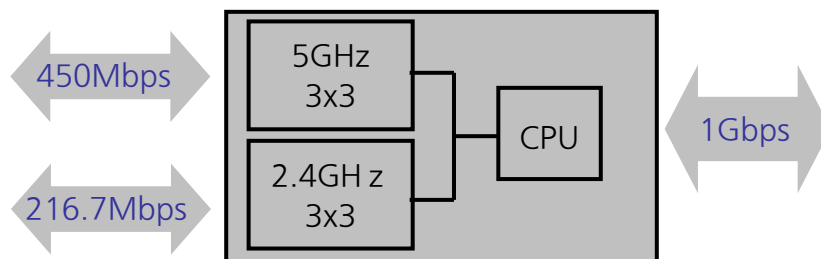



図1.2-1　ハードウェアイメージ

伝送速度の最高速は、規格による理論上の速度であり、ご利用環境や接続機器などにより実際のデータ速度は異なります。

1.2.2.　LTE/3G 網を利用しての無線 LAN 端末データ転送（屋内用無線 LAN アクセスポイントのみ）

屋内用無線 LAN アクセスポイント（EA-7HW01AP1）のみ、LTE/3G 網を利用して L2TP＋IPsec のようなインターネット VPN 接続による無線 LAN 端末データの転送が可能です。

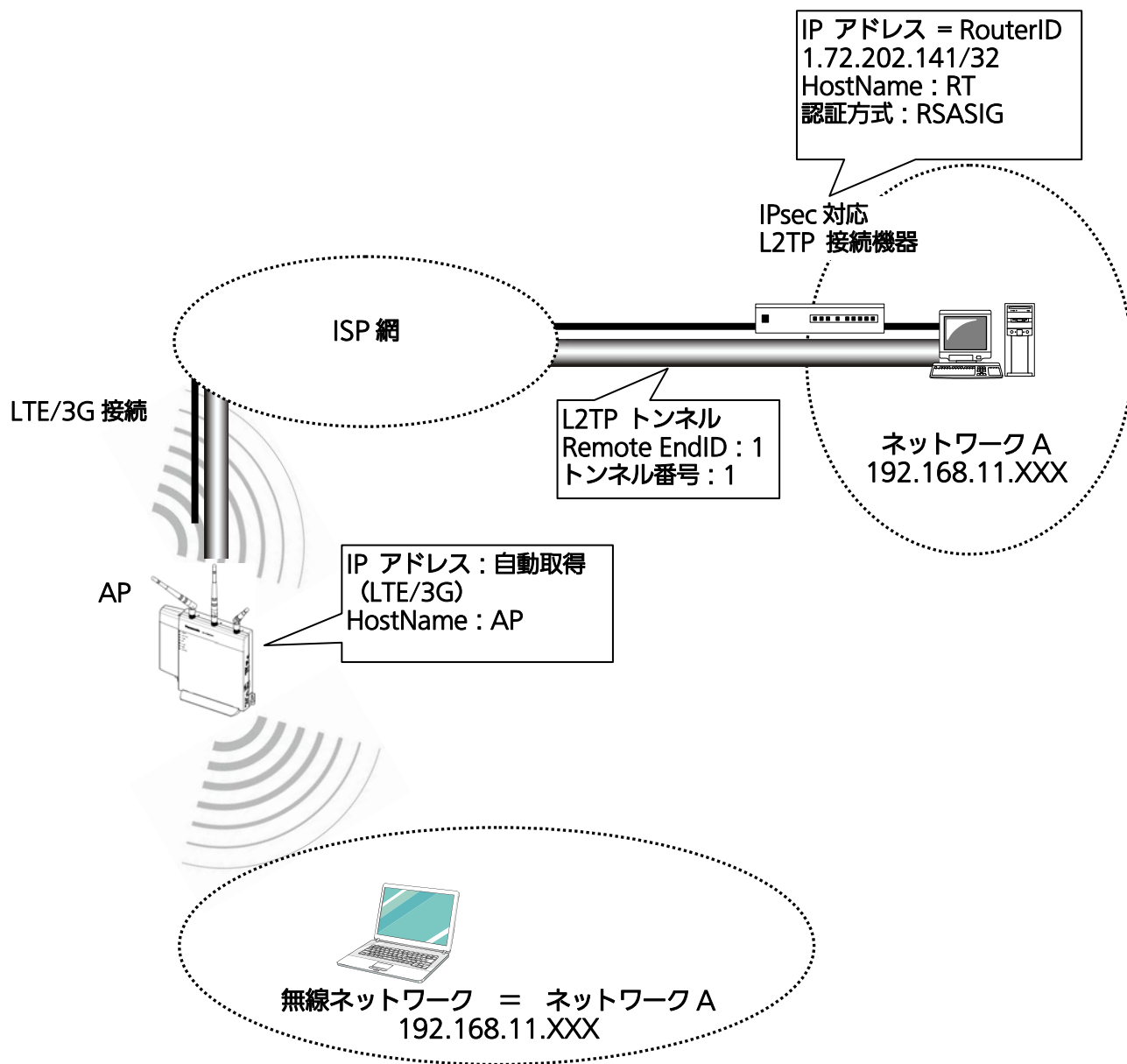



図1.2-2　LTE/3G 接続イメージ

1.2.3.　急増した無線 LAN 端末への対応　ー同時接続 320 台ー

スマートフォンを中心に無線 LAN 対応機器が急速に普及したため、1 台の無線 LAN アクセスポイントへの過密接続が問題となってきました。通信はほとんど行わないものの接続状態となったままの端末が増えることで、最大端末接続台数が数 10 台程度しかない従来の無線 LAN アクセスポイントでは、通信帯域に空きがあっても端末を追加接続することができませんでした。本装置では、無線インターフェースごとに最大 320 台の端末接続を実現し、また接続済の端末台数が一定以上の場合に限り、通信を行っていない端末を積極的に切断するなど、過密接続への課題に対応します。

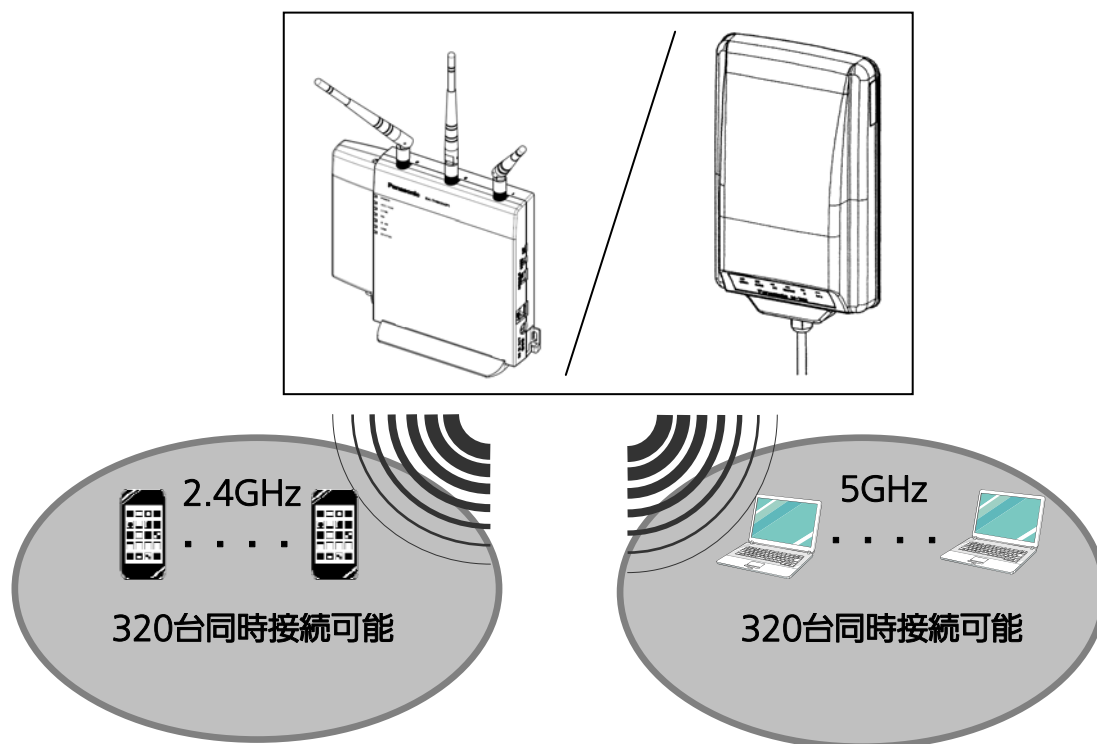



図1.2-3　 同時接続イメージ

1.2.4.　各種 VPN ネットワークへの対応

本装置を設置する場合、駅、飲食店、大規模商業施設などそれぞれの場所によって、アクセス網にも様々な形態が存在します。特にインターネット回線が既に敷設されている場合は、L2TP＋IPsec のようなインターネット VPN 接続により本装置とセンター側を結ぶことがあります。本装置では、従来外部装置で構成していた VPN 機能を内蔵しており、機器コストや設置スペースに起因する運用コストの低減を可能にします。

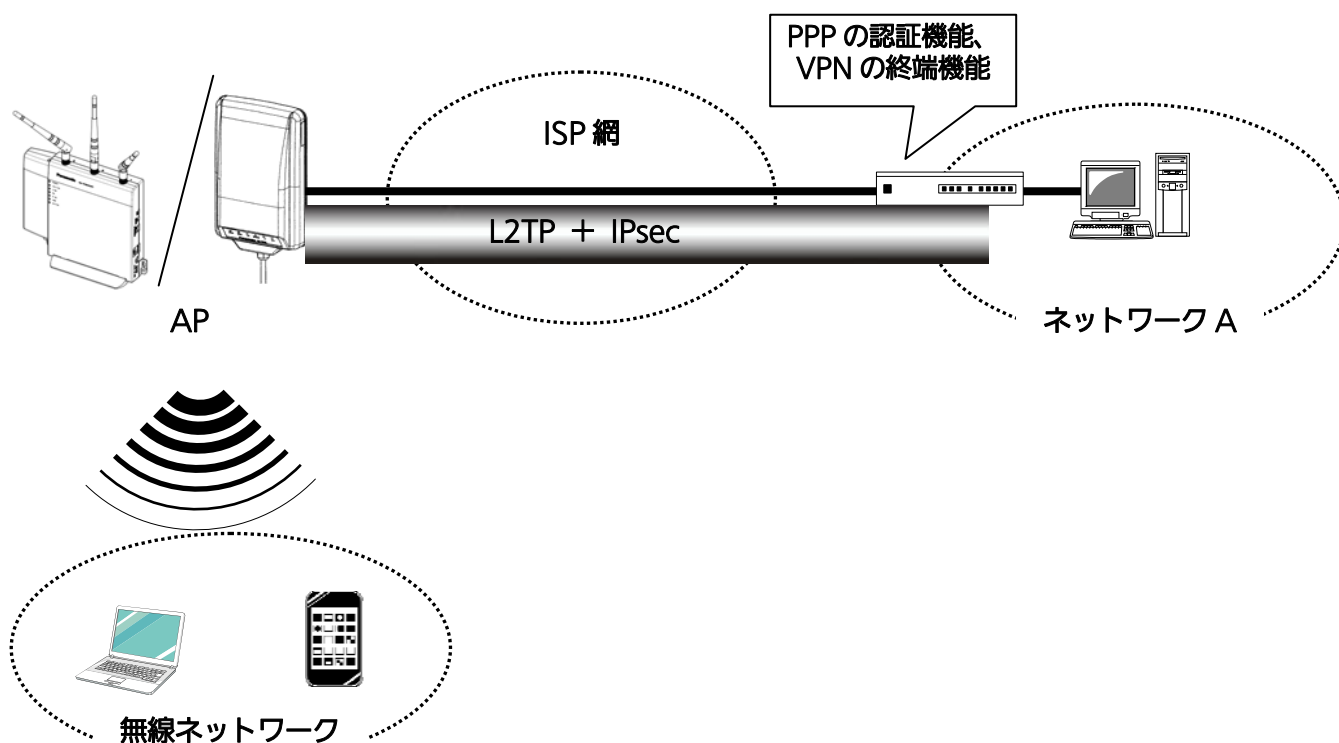



図1.2-4　 VPN 接続イメージ

1.2.5. QoS 機能

本装置が備える QoS 機能は、大きく分けて優先制御と帯域制御の 2 つに分けられます。優先制御は、IP 電話など急ぎのパケットを、出力インターフェースでなるべく待たせずに送り出す技術です。一方の帯域制御は、特定の通信の帯域を確保したり、逆に制限したりする機能です。さらに、上記 2 つの機能を正しく利用するために、受け取った IP パケットを識別する機能を持ちます。これらの機能により、通信品質を保つことができます。

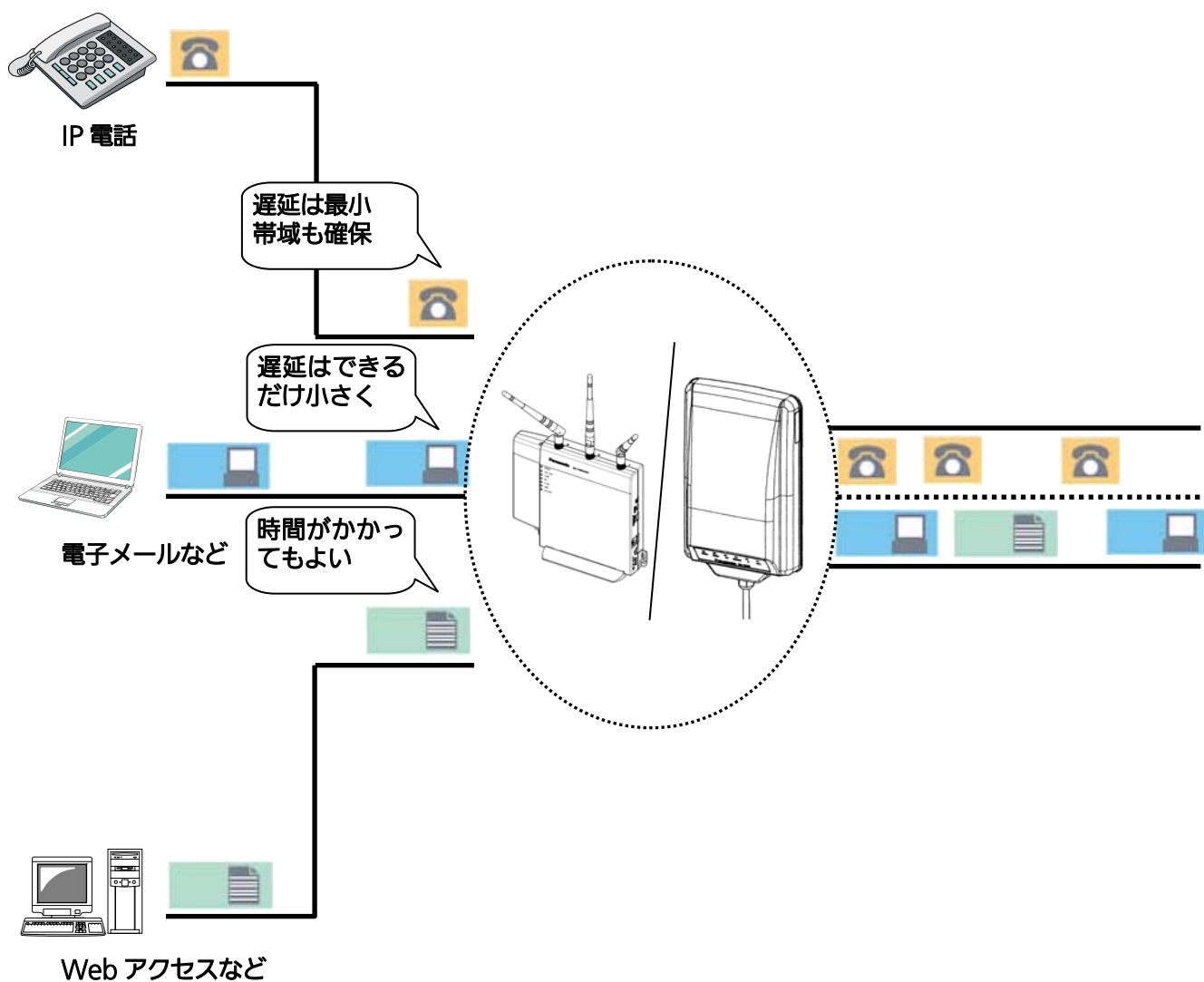



図1.2-5　QoS 機能イメージ

1.2.6. 端末接続制御機能

端末接続制御機能による、特定のアクセスポイントへの端末接続集中を抑止します。SSID ごとに通信端末数の設定値をチューニングすることによって、たとえば、音声の通信要求が発生した際に、データ端末の接続を切断し、音声通信を優先させることができます。

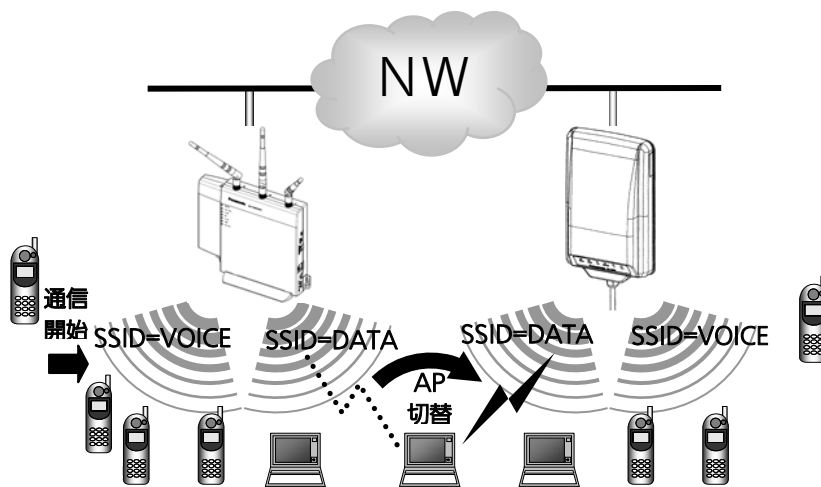



図1.2-6　端末接続制御機能イメージ

1.2.7. 無線ブリッジ機能

無線ブリッジ機能による、LAN 配線が困難な場所等に無線エリア拡張（アクセスポイント間を無線でつなぎます）が可能です。最大 8 分岐の多段接続に対応していますので、広域エリアへの適用も可能です。

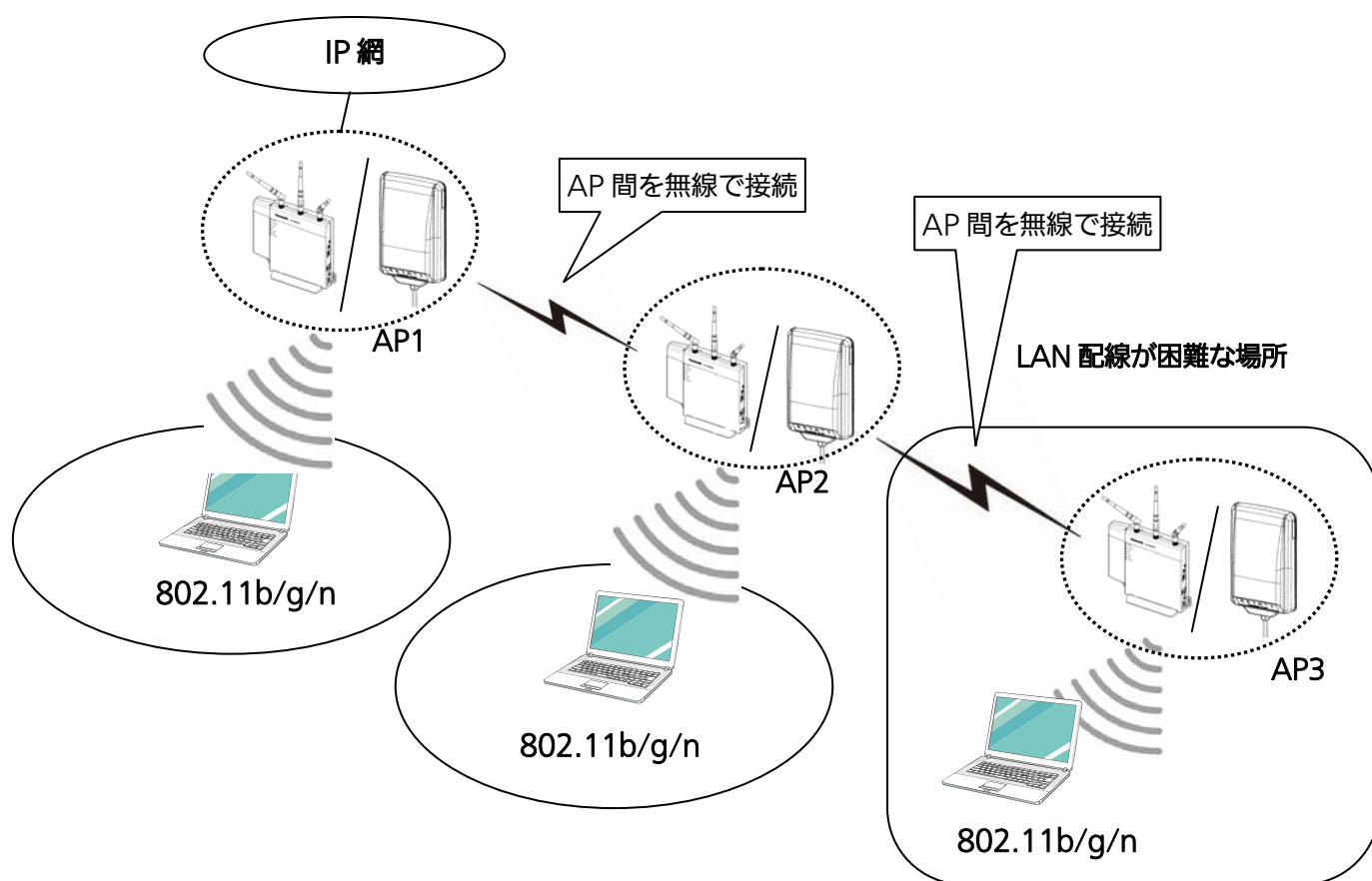



図1.2-7　無線ブリッジ機能イメージ

1.2.8.　多彩な VLAN 機能

SSID ごとの VLAN 分離、ユーザー認証 VLAN に対応しています。

- SSID ごとに VLAN を設定することにより各 SSID のトラフィックを VLAN 分離可能です。
- 端末認証時の認証情報に従った、ユーザー認証 VLAN によりトラフィックを VLAN 分離可能です。
- SSID VLAN およびユーザー認証 VLAN を組み合わせたフレキシブルな VLAN 構成が可能です。

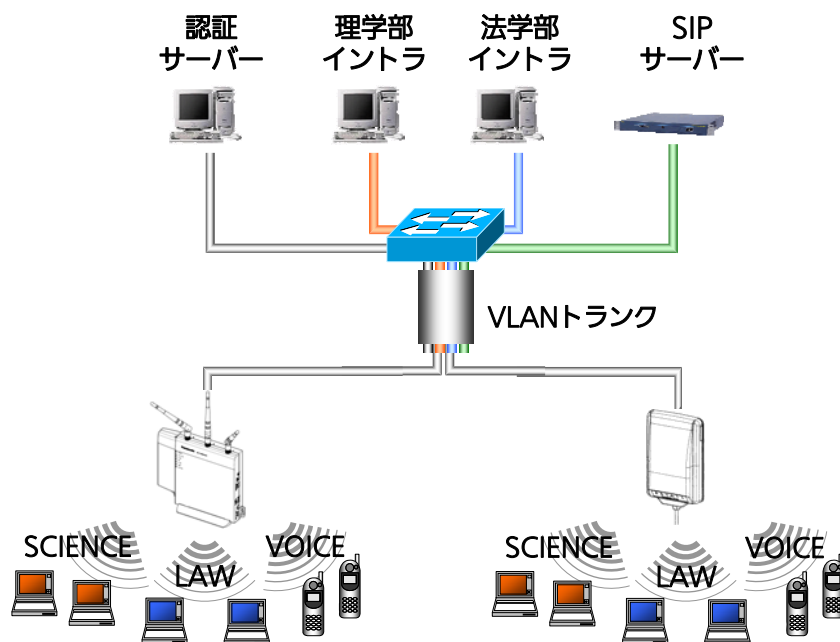



図1.2-8　　VLAN 機能イメージ

1.2.9.　解析機能強化 －統計情報管理・パケットログ－

本装置は、サービス事業者ごと（SSID 単位）に端末の接続状況やトラフィックなどのユーザー利用状況の把握が可能です。一定周期でアソシエーション成功／失敗の端末数、送受信したパケット数やバイト数などの情報を蓄積し、色々な分析や解析に利用できます。
また、アソシエーションから IEEE802.1X 認証完了までの本装置～端末間の接続シーケンスをパケットレベルで記録・保存する機能を持ち、接続問題の解析に活用できます。

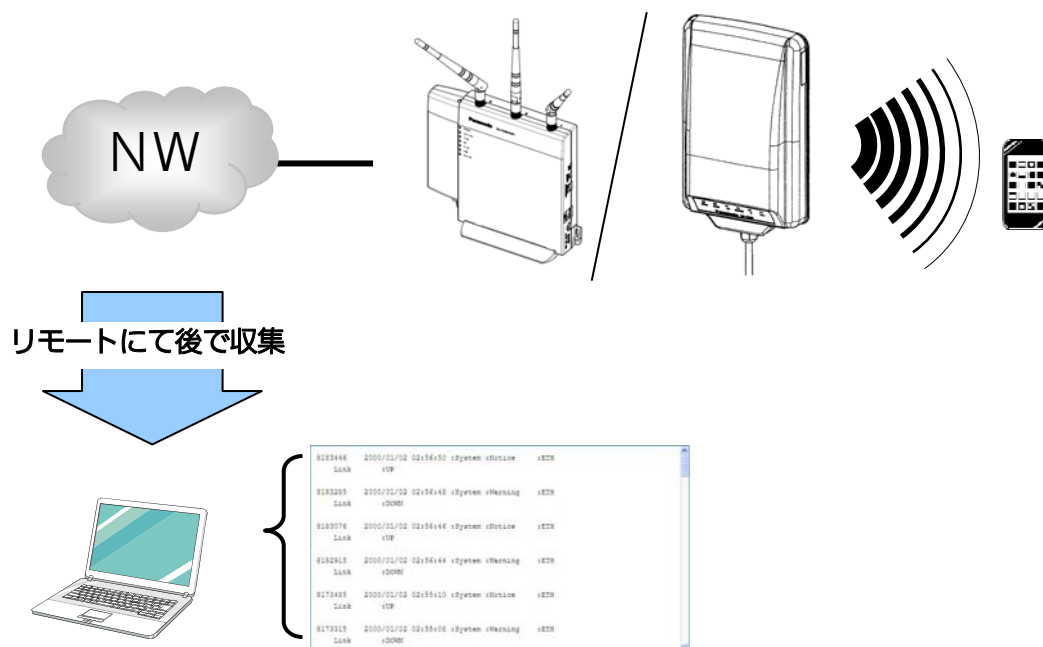



図 1.2-9　パケットキャプチャイメージ

1.2.10.　サービス品質向上の対応

本装置ではサービス品質向上のため、以下の機能も実装しております。

- 5GHz 帯域への誘導
- 低電界端末の接続拒否による、通信状態の安定化
- 同時端末接続数制御
- 最低接続保証台数制御
- IGMP スヌーピング
- Passpoint 対応

詳細は、4.7　サービス品質向上機能をご参照ください。

第 2 章　設定の準備

本装置設定のための準備について説明します。

2.1　Webコンソール用パソコンの設定

Web コンソールを利用する際に使用する、Web コンソール用パソコンの接続方法と本装置の設定について説明します。

表2.1-1　　Web コンソール用パソコンの推奨環境

OS および TCP/IP ソフトウェア	Microsoft®　Windows®　XP Microsoft®　Windows　Vista® Microsoft®　Windows®　7 TCP/IP ソフトウェアは OS に付属しています。別途ご用意いただく必要はありません。
画面解像度	1024 x 768 ピクセル以上
LAN カード	本装置とパソコンを接続するために、パソコンに Ethernet ポートが必要です。LAN カードを使用する場合は、ご使用になるパソコンに装着できる LAN カードをご用意ください。
WWW ブラウザ	本装置の設定に Web コンソールを使用する際には、以下の WWW ブラウザをご用意ください。 ・Windows®　Internet Explorer 8.0®以上 ※同一端末で複数ブラウザ画面からのアクセスには対応しておりません。

◆LAN カードの準備

Web コンソール用パソコンに Ethernet ポートがあることを確認してください。Ethernet ポートがないパソコンの場合は、LAN カードを装着する必要があります。LAN カードを新規に装着した場合には、LAN カードのソフトウェア（ネットワークドライバ）のインストールが必要となります。パソコンや LAN カードに添付されたマニュアルに従って正しく設定してください。

◆TCP/IP プロトコルの設定

Web コンソールを使用するには、Web コンソール用パソコンで IP アドレスおよびサブネットマスクの設定を済ませておくことが必要です。
設定の手順はパソコンの OS によって異なります。本書では、Microsoft® Windows®　7 を例に説明します。

パソコンに TCP/IP がインストールされていることを確認します。

設定手順

手順1　〔コントロールパネル〕ウインドウを開き、〔ネットワークと共有センター〕をクリックします。
手順2　〔アダプターの設定の変更〕をクリックします。〔ネットワーク接続〕が表示されます。
手順3　〔ローカルエリア接続〕をダブルクリックします。〔ローカルエリア接続のプロパティ〕ダイアログボックスが表示されます。
手順4　一覧にインターネット プロトコル バージョン 4 (TCP/IPv4)が含まれていることを確認します。
一覧にインターネット プロトコル バージョン 4 (TCP/IPv4) が表示されていない場合は、TCP/IP のインストールが必要です。Microsoft® Windows®　7 のマニュアルを参照して、インストールしてください。

図2.1-1　　ローカルエリア接続のプロパティ

手順5　一覧から〔インターネット プロトコル バージョン 4 (TCP/IPv4)〕をクリックして選択し、〔プロパティ〕ボタンをクリックします。

手順6　パソコンの IP アドレスを設定します。設定する IP アドレスとサブネットマスクは、本装置に設定されている IP アドレスとサブネットマスクと整合性をとるように設定してください。本装置の IP アドレスの初期値は、表 2.1-2 に記載します。

表2.1-2　IP アドレス（初期値）

IP アドレス	192.168.0.3
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.0.1

例として、下記内容での設定を示します。

- 〔次の IP アドレスを使う〕を選択
- IP アドレスに「192.168.0.10」を入力
- サブネットマスクに「255.255.255.0」を入力
- デフォルトゲートウェイは入力なし

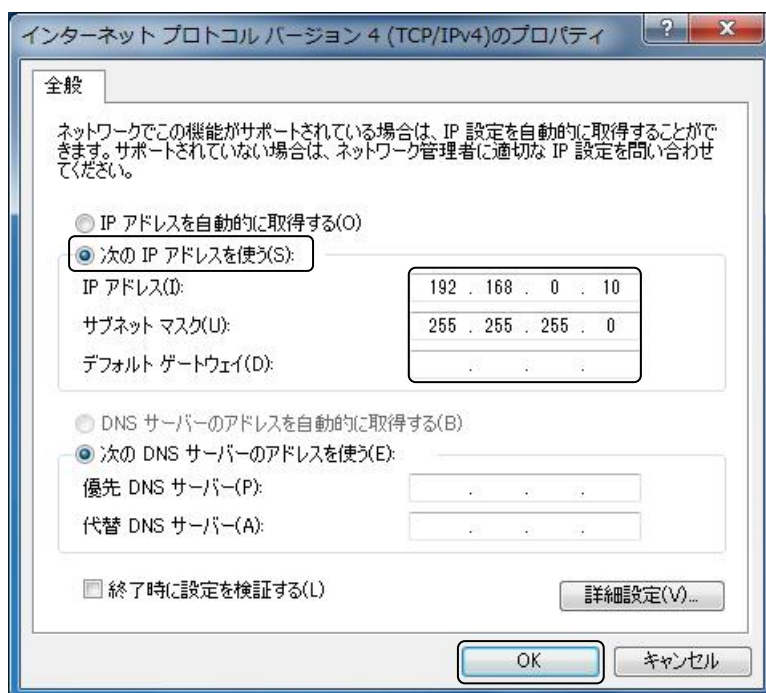



図2.1-2　インターネット プロトコル バージョン 4（TCP/IPv4）のプロパティ

手順7　〔OK〕ボタンをクリックして、〔ローカルエリア接続のプロパティ〕に戻ります。
手順8　〔閉じる〕ボタンをクリックして、〔ローカルエリア接続の状態〕に戻ります。
手順9　〔閉じる〕ボタンをクリックします。

◆WWW ブラウザの準備
設定の手順はパソコンの OS によって異なります。本書では、Microsoft® Windows® 7 を例に説明します。

設定手順

手順1　〔コントロールパネル〕ウインドウを開き、〔インターネットオプション〕をクリックします。〔インターネットのプロパティ〕ダイアログボックスが表示されます。
手順2　〔接続〕タブを選択し、〔LAN の設定〕ボタンをクリックします。
手順3　〔プロキシサーバーを使用する〕がチェックされていないことを確認します。

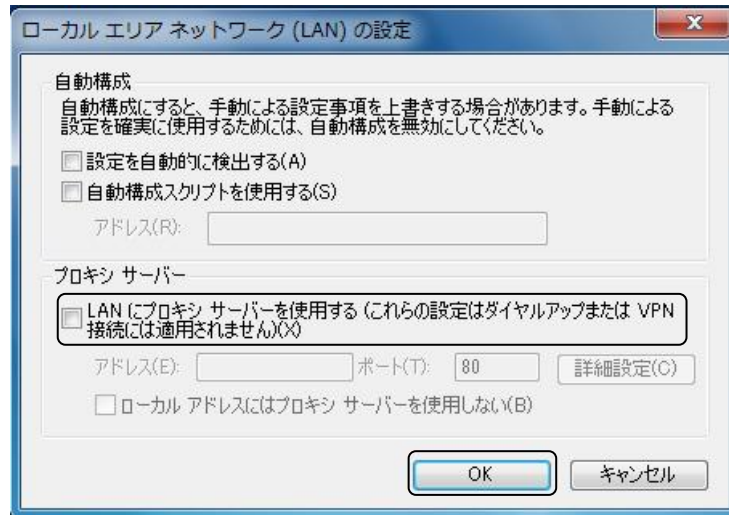



図2.1-3　ローカルエリアネットワークの設定（LAN）

プロキシサーバーを利用する場合は、本装置だけプロキシの対象外として設定してください。

手順4　〔コントロールパネル〕ウインドウを開き、〔インターネットオプション〕をクリックします。〔インターネットのプロパティ〕ダイアログボックスが表示されます。
手順5　〔接続〕タブを選択し、〔LAN の設定〕ボタンをクリックします。
手順6　〔LAN にプロキシサーバーを使用する〕をチェックし、〔詳細設定〕ボタンをクリックします。
手順7　例外の〔次で始まるアドレスにはプロキシを使用しない〕に本装置の IP アドレスを指定します。
手順8　〔OK〕ボタンをクリックして、〔ローカルエリアネットワーク（LAN）の設定〕に戻ります。
手順9　〔OK〕ボタンをクリックして、〔インターネットのプロパティ〕に戻ります。
手順10　〔OK〕ボタンをクリックします。

2.2　Webでのログイン・ログアウト

◆ユーザー種別

ユーザーカウントには、管理ユーザーと一般ユーザーの 2 種類があります。それぞれについては、表 2.2-1 にまとめています。

表2.2-1　ユーザー種別

	ユーザー名	パスワード	権限
管理ユーザー	root	root	すべての操作が可能
一般ユーザー	user	user	設定や状態の表示のみ可能

重要	■ ユーザー名・パスワードは初期値の設定から必ず変更し、適正に管理してください。ユーザー名・パスワードの変更方法については、 「2.3 ユーザー名・パスワードの変更」を参照してください。

◆ログイン

WWW ブラウザに表 2.1-2 の IP アドレスを入力すると、ログイン画面（図 2.2-1）が表示されます。
ユーザー種別（表 2.2-1）のユーザー名とパスワードを入力してください。

図2.2-1　ログイン画面

ユーザー名とパスワードが正しい場合、Web コンソールメイン画面（図 2.2-2）が表示され、該当するユーザーレベルでのコンソール操作が可能となります。
また、本装置のアカウントは、ユーザー権限に関わらず、1 つのアカウントのみ使用できます。

図2.2-2　Web コンソールメイン画面

◆ログアウト

Web コンソール画面の右上の〔ログアウト〕をクリックしてください。

図2.2-3　Web コンソールメイン画面（ログアウト）

画面を閉じるか確認するダイアログが表示されますので、〔はい〕を選択して画面を閉じてください。

また、IP の変更を行った場合自動でログアウトされます。

2.3 ユーザー名・パスワードの変更

本装置へのログインに必要なアカウント情報（ユーザー名・パスワード）は、それぞれ[ユーザー名：0～16文字（英・数字）]、[パスワード：0～16 文字（英・数字）]にて設定することができます。

◆ユーザー名変更

Web コンソールでのユーザー名の変更に関する設定は以下の通りです。

設定手順

手順1　〔保守〕　→　〔ユーザー名変更〕を選択します。

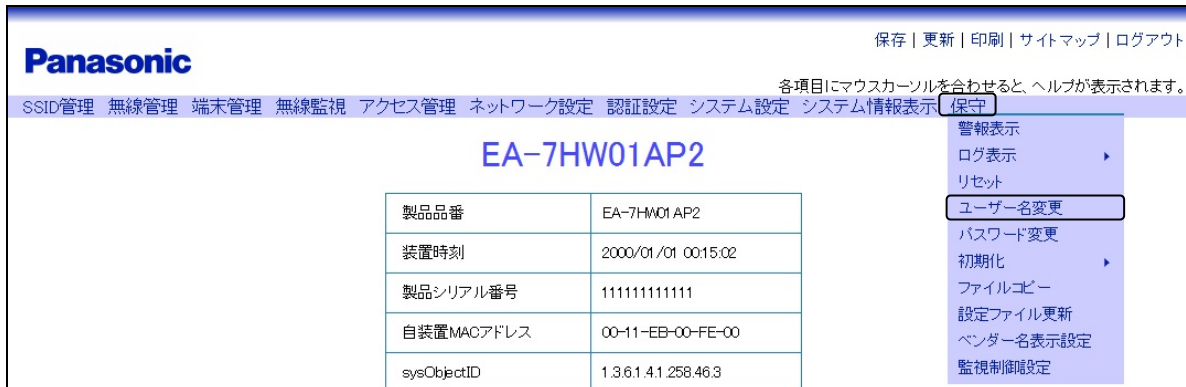



図2.3-1　メニュー（ユーザー名変更）

手順2　ユーザー名を変更します。

例として、下記内容での設定を示します。

・　ユーザー種別：〔一般ユーザー〕を選択

・　ユーザー名：「user01」を入力

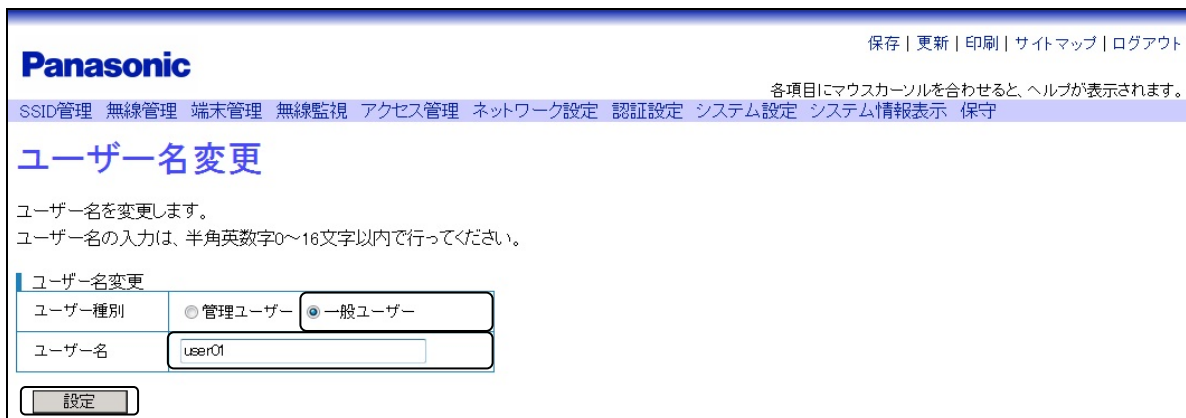



図2.3-2　ユーザー名変更

手順3　編集が完了したら、〔設定〕ボタンをクリックします。

◆パスワード変更

Web コンソールでのパスワードの変更に関する設定は以下の通りです。

手順1　〔保守〕　→　〔パスワード変更〕を選択し、パスワードを変更します。

例として、下記内容での設定を示します。

- ユーザー種別：〔一般ユーザー〕を選択
- 古いパスワード～新しいパスワード（確認用）を入力

図2.3-3　パスワード変更

手順2　編集が完了したら、〔設定〕ボタンをクリックします。

重要	■ ユーザー名およびパスワードを変更する場合、管理ユーザーでログインしておく必要があります。 ■ 管理ユーザー変更後の設定は厳重に管理願います。変更後の設定がわからなくなった場合、ログインによる再設定ができません。 ■ セキュリティー上、初期設定時は「管理ユーザー」「一般ユーザー」のアカウント情報を変更するようお願いいたします。

2.4　CLIコンソールでのログイン・ログアウト

本装置の各種設定を行う方法には、Web コンソールの他に、CLI コンソール　（コマンドライン・インターフェース・コンソール）があります。ここでは、CLI コンソールの準備、ログイン・ログアウト方法について説明します。

◆コンソールの接続方法

コンソールとは、通信ソフトがインストールされているパソコンなどを指します。本装置とコンソールを接続するには、USB ケーブルでコンソールポートとシリアル接続する方法（屋内用無線 LAN アクセスポイントのみ）と、Ethernet ケーブルで接続し、ネットワーク経由で Telnet によりリモートログインする方法があります。

USBケーブルで接続する場合、あらかじめコンソール用PCにドライバをインストールしておく必要があります。ドライバはパナソニックビジネスサイト（http://panasonic.biz/netsys/wifi）からダウンロードしてください。

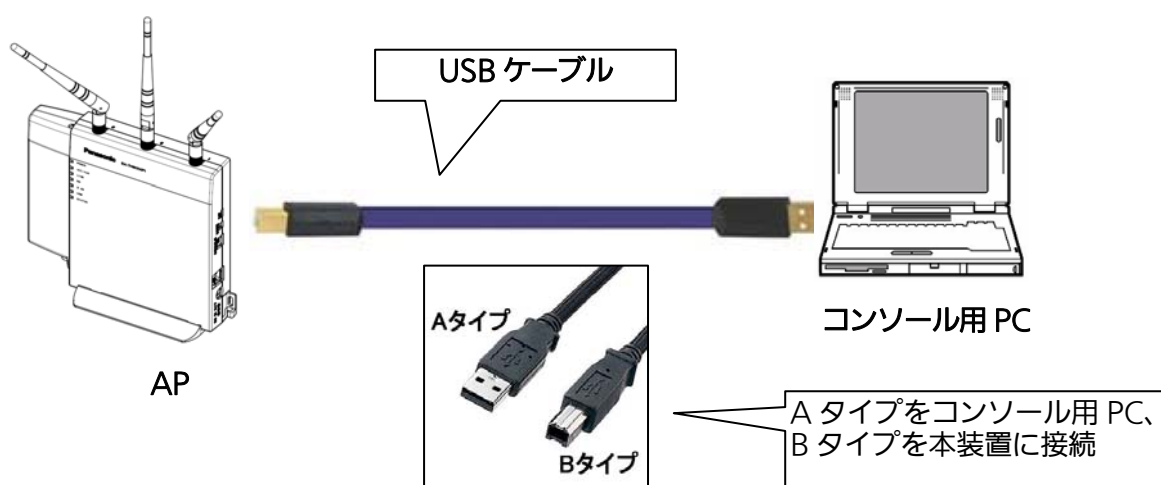



図2.4-1　　コンソール接続例（USB ケーブル）

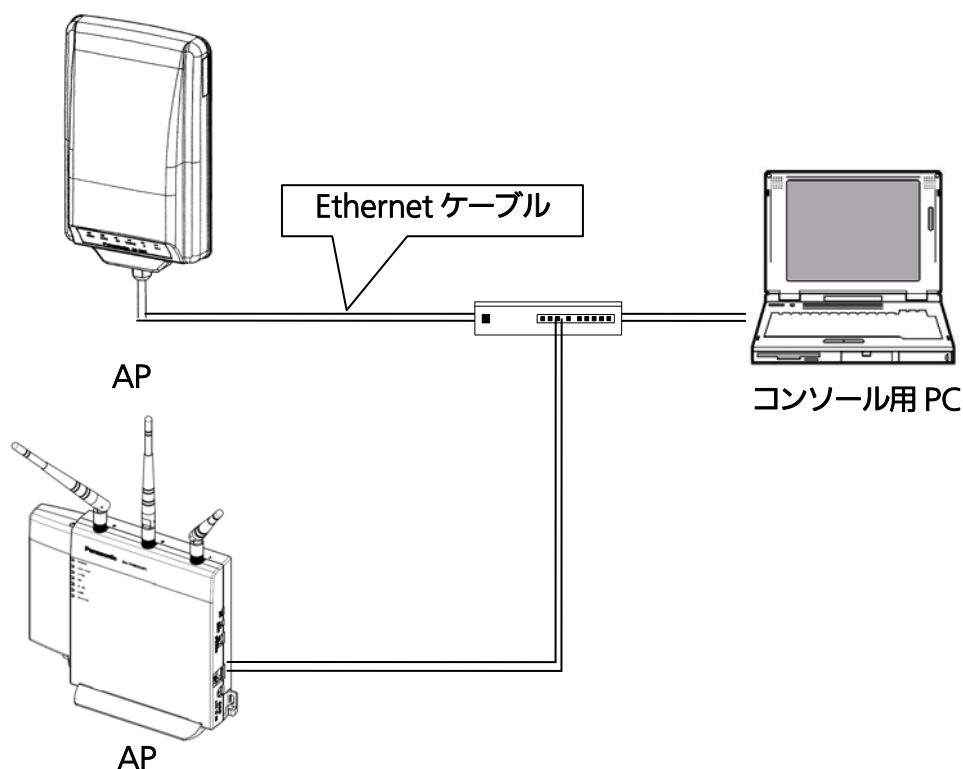



図2.4-2　　コンソール接続例（Telnet）

◆USB ドライバインストール手順（屋内無線 LAN アクセスポイントのみ）
本書では、Microsoft® Windows®　7 を例に説明します。
※コンソール用 PC に以下の権限のユーザーでログインしてください。
　Microsoft®　Windows®　7/ Microsoft®　Windows　Vista®：「管理者」権限をもつユーザー
　Microsoft®　Windows®　XP：「コンピュータの管理者」権限をもつユーザー

手順1　ダウンロードしたファイルをダブルクリックします。〔セキュリティの警告〕画面が表示されるので〔実行（R)〕をクリックします。

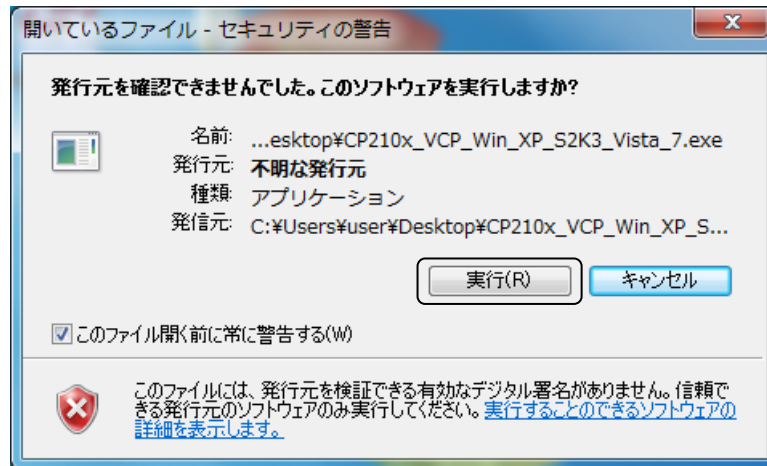



図2.4-3　セキュリティの警告

手順2　〔InstallShield Wizard〕画面が表示されるので〔Next > 〕をクリックします。

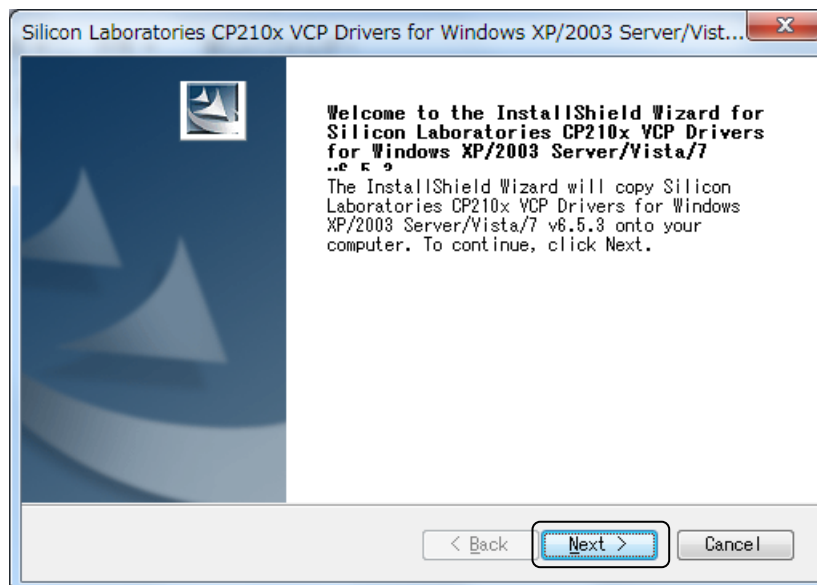



図2.4-4　InstallShield Wizard

手順3　〔License Agreement〕画面が表示されます。ライセンス条件をご確認の上、〔I accept the terms of the license agreement〕をクリックし、〔Next > 〕をクリックします。

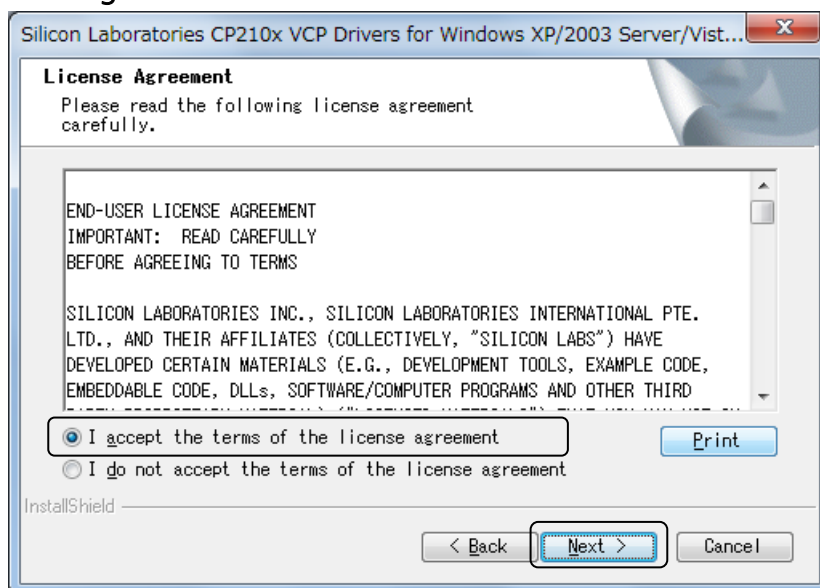



図2.4-5　License Agreement

手順4　〔Choose Destination Location〕画面が表示されるのでインストール先のディレクトリを変更する場合は〔Browse...〕をクリックしインストール先を指定後、〔Next > 〕をクリックします。

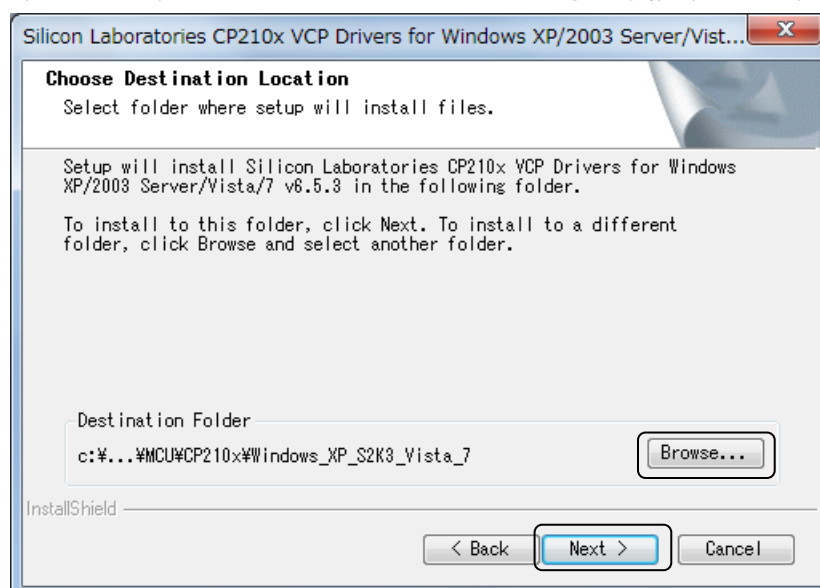



図2.4-6　Choose Destination Location

手順5　〔Ready to Install the Program〕画面が表示されるので〔Install〕をクリックします。

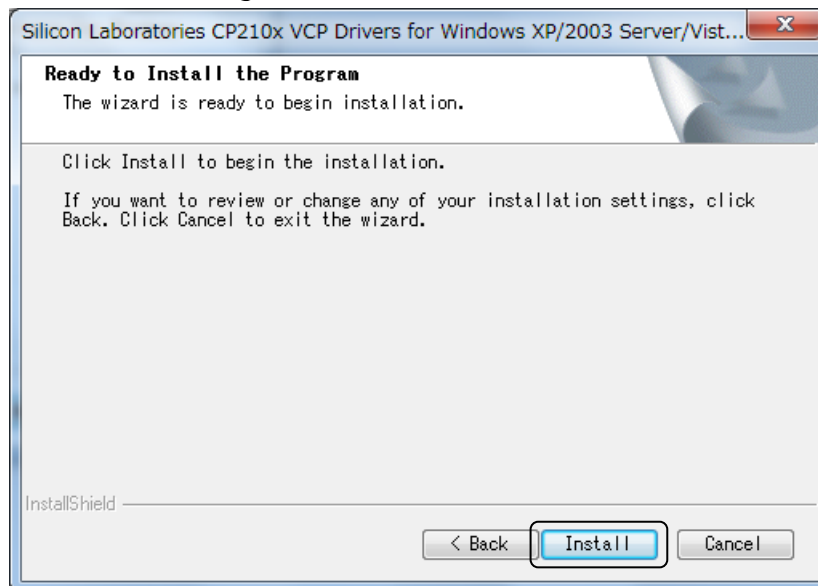



図2.4-7　Ready to Install the Program

手順6　〔Setup Status〕画面が表示され、インストールを開始します。

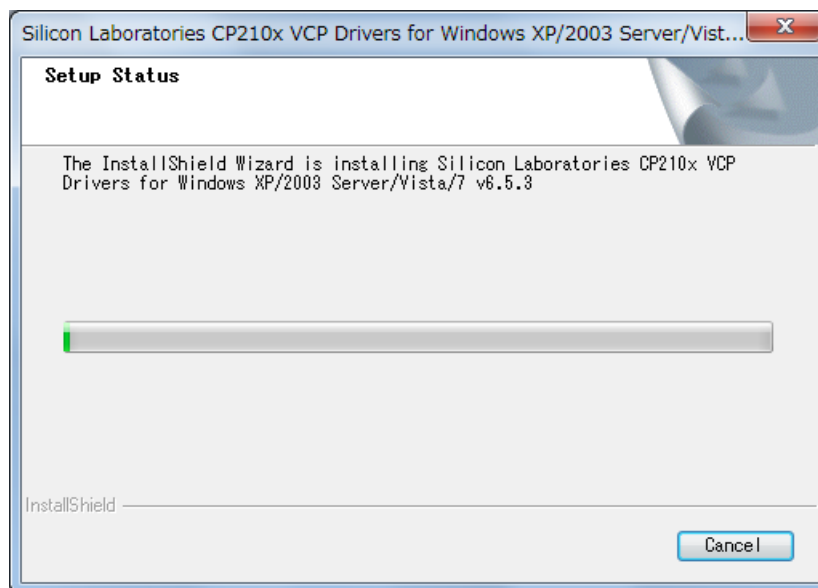



図2.4-8　Setup Status

手順7　〔InstallShield Wizard Complete〕画面が表示されるので、〔Finish〕をクリックします。

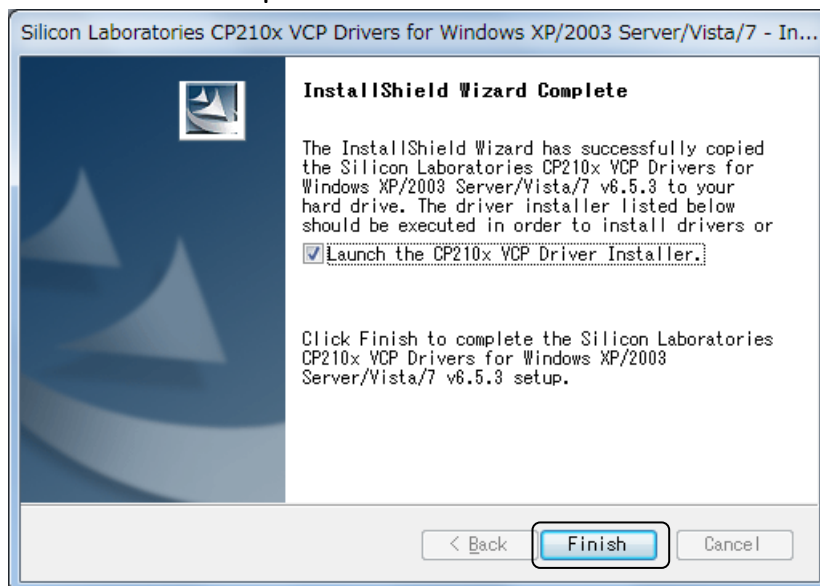



図2.4-9　InstallShield Wizard Complete

手順8　〔Silicon Laboratories〕画面が表示されるので、〔Install〕をクリックします。

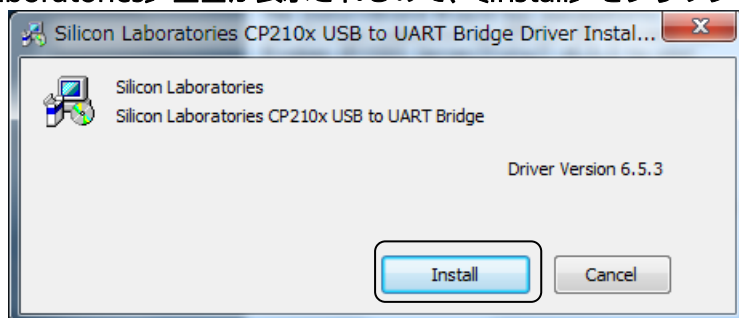



図2.4-10　Silicon Laboratories

手順9　〔Success〕画面が表示されるので、〔OK〕をクリックします。

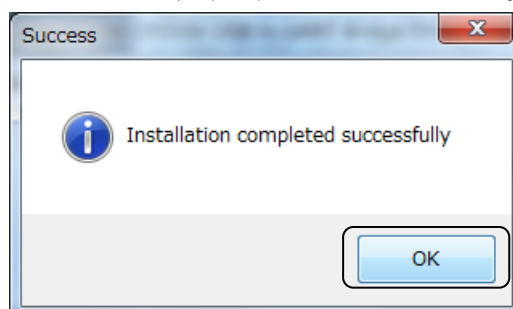



図2.4-11　Success

以上でドライバのインストールは終了です。

◆シリアル接続コンソールの通信ソフト設定

通信ソフトの例として、フリーウェアで「Tera Term」があります。 コンソール用 PC 上の通信ソフトを起動して、シリアルポートの設定を以下のように設定してください。

表2.4-1 コンソールの通信ソフト設定

設定項目	内容
シリアルポート	本装置と接続しているポート番号
通信速度（ボー・レート）	115200 bit/s
データ長	8 bit
パリティ	なし
ストップビット	1 bit
フロー制御	なし

CLI コンソールのログイン・ログアウト方法について説明します。

◆コンソール画面の表示

コンソール用 PC 上の通信ソフトを起動して、本装置とシリアル接続または TCP/IP 接続を行ってください。
通信ソフトの画面が以下のように表示されたら、接続は完了です。

```
Login  :
       ↑  ユーザー名入力待ちになります。
```

◆ユーザー種別

ユーザー名、パスワードについては、「2.2 ユーザー名とパスワードの変更」を参照してください。

◆ログイン

ユーザー名とパスワードを入力してください。ユーザー名とパスワードが正しい場合、該当するユーザーレベルのプロンプトが表示され、コンソールの操作が可能となります。

```
Login      : root
Password   : *****
             ↑  管理ユーザーのユーザー名、パスワードを入力します。（例）
#
↑  管理ユーザーのプロンプトを表示します。
```

◆ログアウト

ログアウトコマンドを入力してください。ログアウトコマンドを入力後、通信ソフトが終了します。
本装置の不正操作を防ぐために、操作をしない時は必ずログアウトをしてください。

```
# exit
  ↑  ログアウトコマンドを入力します。
```

第３章　装置の基本設定

本装置の基本的な設定を行うための手順について、説明します。

3.1　基本設定の流れ

本装置の基本的な設定は、以下の手順で行います。

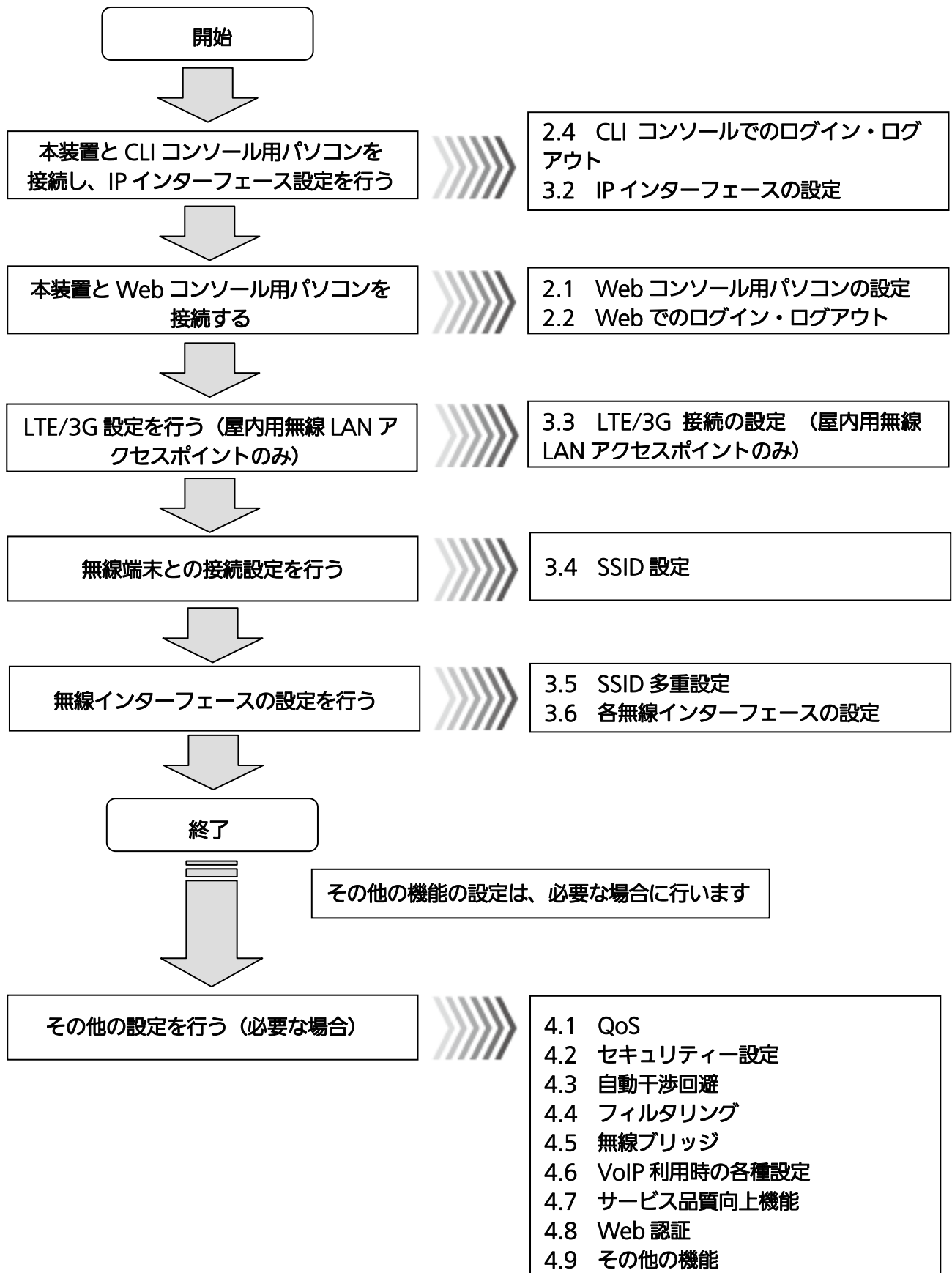



図3.1-1　　ネットワーク構成手順

ここでは、下図の「営業部門用ネットワーク」へ接続する場合の設定を紹介します。

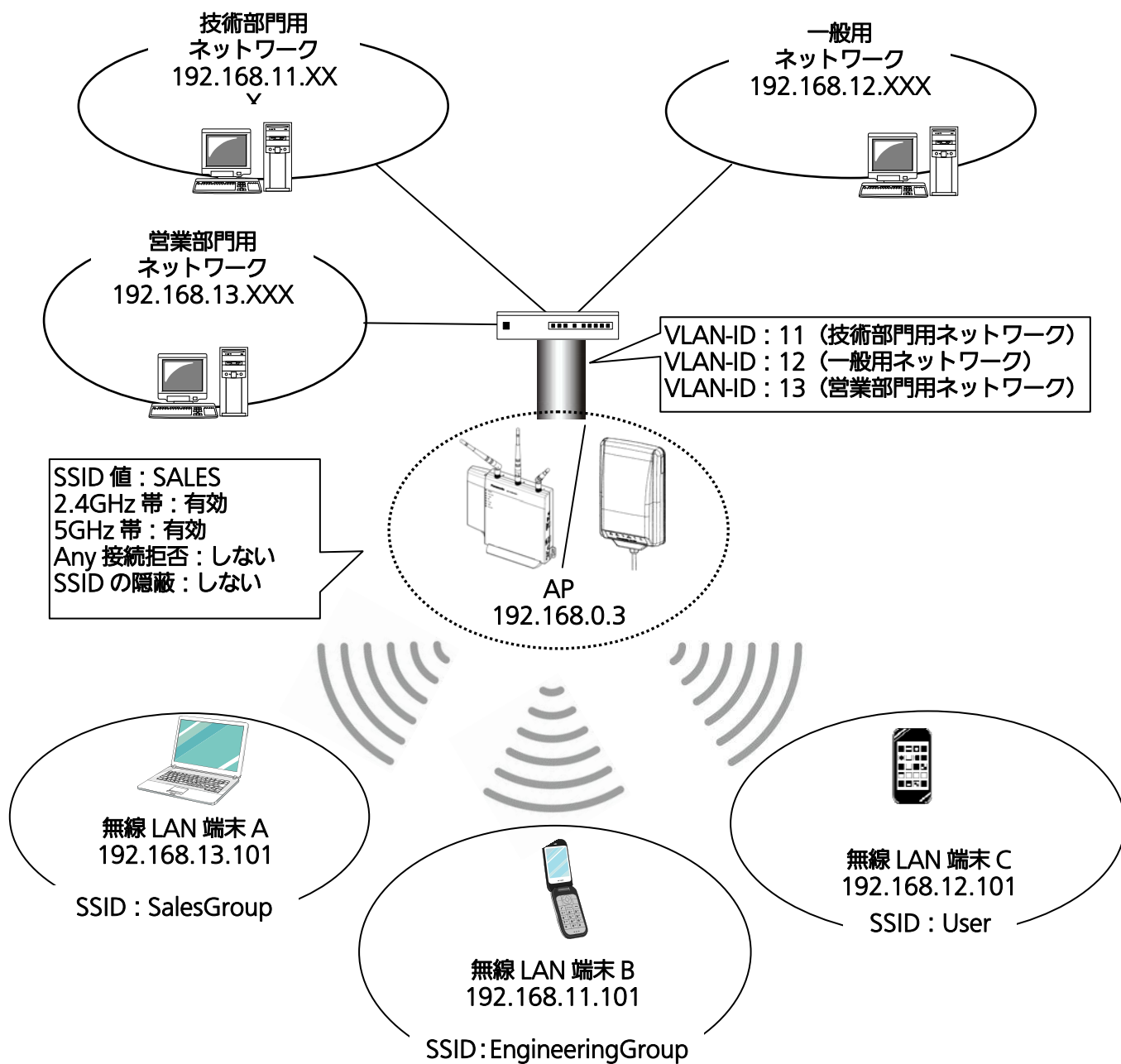



図3.1-2　ネットワーク構成例

Web コンソールを使用した本装置の各設定値の確定、設定データの保存、リセット（自装置の再起動）について説明します。

操作手順

◆設定値の確定

各設定画面で行った設定を確定させるために、必ず各設定画面左下の〔設定〕ボタンをクリックしてください。

手順1　各設定画面左下の〔設定〕ボタンをクリックし、設定を確定します。

戻る　設定

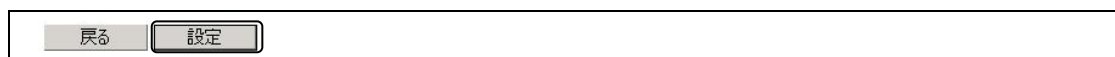



図3.1-3　設定ボタン

- クリック後にエラーポップアップが出た場合は、設定漏れなどの可能性があるので、画面右上の〔更新〕をクリックし、最新の設定状態を画面で確認してください。

図3.1-4　設定の更新

◆設定データの保存

設定が完了したら、最後に必ず設定データを保存します。

手順1　画面右上の〔保存〕をクリックし、設定した内容を本装置に保存します。

図3.1-5　設定の保存

重要	■　設定データの保存処理中は、絶対に装置の電源を切らないでください。

◆リセット

自装置を再起動する手順を説明します。

手順1　〔保守〕　→　〔リセット〕を選択します。

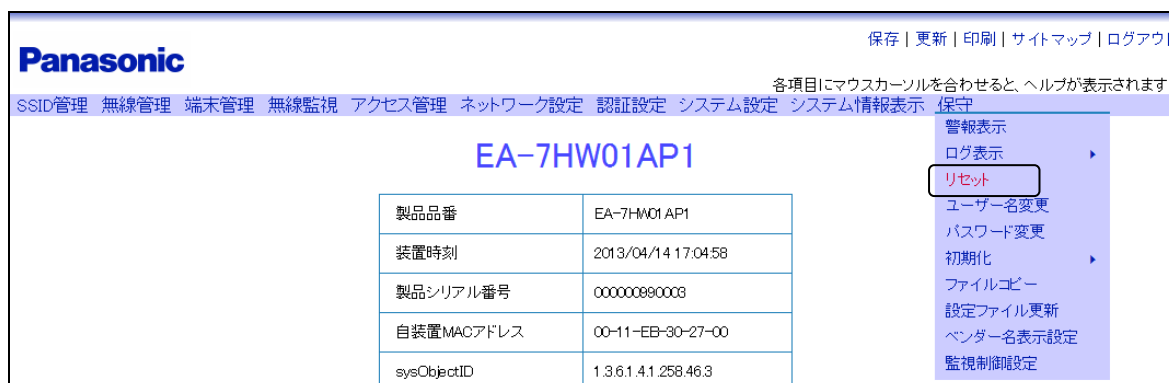



図3.1-6　リセット

手順2　〔自装置再起動〕の実行ボタンをクリックします。

図3.1-7　自装置再起動

手順3　ポップアップ画面のＯＫボタンをクリックすると、装置が再起動します。

図3.1-8　ポップアップ画面

3.2　IP インターフェースの設定

ここでは、ネットワークに本装置を接続するための基本的な設定方法を説明します。

本装置はマルチプル IP 対応により、IP アドレスを 16 個まで設定することが可能で、それぞれ独立した管理系ネットワークに所属させ監視・保守を行うことができます。各 IP インターフェースに設定する IP アドレスは、固定的設定に加えて DHCP プロトコルを使用することにより、DHCP サーバーから IP アドレスを取得することができます。
また、各 IP インターフェースが所属する管理系ネットワークの VLAN 設定も行うことができます。

設定手順

◆IP アドレスの設定
例として、IP インターフェース 1 番に対して設定を行います。IP アドレス設定には CLI コンソールを使用します。

手順1　管理ユーザーでログインします。

```
Login      : root
Password    : *****

#
```

手順2　IP インターフェース 1 番を有効にします。

```
# admin ip status 1 enabled

#
```

手順3　IP インターフェース 1 番の動作モードを〔static〕にします。

```
# admin ip mode 1 static

#
```

動作モードは以下の通りとなります。
static　　：IP アドレス固定（static）動作
dhcp　　：IP アドレス取得（DHCP）動作
ppp　　：IP アドレス取得（PPP）動作

動作モード設定が「dhcp」で DHCP サーバーと通信が出来なかった場合、「static」設定の設定値が反映されます。（IP インターフェース 1 番はあらかじめ、初期値：192.168.0.3 が入力されていますので、DHCP サーバーと通信が出来なかった場合は、IP アドレス＝192.168.0.3 で運用します）

手順4　IP インターフェース 1 番に対して IP アドレスを設定します。

例として、下記内容での設定を示します。

・ IP アドレスに「192.168.0.3」を入力
・ サブネットマスクに「255.255.255.0」を入力
・ デフォルトゲートウェイに「192.168.0.1」を入力

```
# admin ip set 1 192.168.0.3 255.255.255.0 192.168.0.1

#
```

設定手順

◆VLAN（Admin VLAN）の設定

例として、IP インターフェース 1 番に対して設定を行います。VLAN 設定には CLI コンソールを使用します。

手順1　IP インターフェース 1 番に対して VLAN-ID、CoS 値を設定します。

例として、下記内容での設定を示します。

・ VLAN-ID :「11」、CoS 値 :「7」を入力

```
# admin vlan vlanid 1 vlanid 11

# admin vlan cos 1 7

#
```

手順2　IP インターフェース 1 番に対して VLAN モードを設定します。

例として、下記内容での設定を示します。

・ VLAN モード :〔シングルタグ〕を選択

```
# admin vlan mode 1 singletag

#
```

重要	■ IP インターフェース設定変更完了後は、Web コンソール用パソコン側のネットワーク、VLAN 設定を無線 LAN アクセスポイントの設定に合わせて変更してください。設定した値によっては、以降の接続ができなくなりますのでご注意ください。 ■ 同時に設定可能な PPP 接続は 1 つです。 ■ IP の変更を行った場合、Web ログイン、Telnet ログインは自動でログアウトされます。

3.3　LTE/3G 接続の設定　（屋内用無線 LAN アクセスポイントのみ）

ここでは、本装置で LTE/3G 接続するための基本的な設定方法を説明します。LTE/3G 接続は屋内用無線 LAN アクセスポイント（EA-7HW01AP1）のみ可能です。屋内用無線 LAN アクセスポイント（EA-7HW01AP1）を LTE/3G 接続しないで、Ethernet 接続で使用する場合、本設定は不要です。

設定手順

下記手順 1 ～9 は、LTE/3G 接続設定を行う場合に Web コンソールでログインするために使用する IP インターフェースの設定です。LTE/3G 接続する IP インターフェースと Web コンソールでログインする IP インターフェースは同一番号の IP インターフェースを使用できません。そのため、下記手順 1 ～9 にて Web コンソールでログインする IP インターフェース設定を行い、手順 10 以降で LTE/3G 接続設定を行います。

◆IP アドレスの設定

IP インターフェース 2 番に対して設定を行います。IP アドレス設定には CLI コンソールを使用します。

手順1　　管理ユーザーでログインします。

```
 Login        : root
 Password     : *****

#
```

手順2　　IP インターフェース 2 番の動作モードを〔static〕にします。

```
# admin ip mode 2 static

#
```

手順3　　IP インターフェース 2 番に対して IP アドレスを設定します。

例として、下記内容での設定を示します。

・　IP アドレスに「192.168.0.100」を入力
・　サブネットマスクに「255.255.255.0」を入力
・　デフォルトゲートウェイに「192.168.0.1」を入力

```
# admin ip set 2 192.168.0.100 255.255.255.0 192.168.0.1

#
```

◆VLAN（Admin VLAN）の設定

IP インターフェース 2 番に対して設定を行います。VLAN 設定には CLI コンソールを使用します。

手順4　IP インターフェース 2 番に対して VLAN-ID を設定します。

例として、下記内容での設定を示します。

・ VLAN-ID :「100」を入力

```
# admin vlan vlanid 2 vlanid 100

#
```

手順5　IP インターフェース 2 番に対して VLAN モードを設定します。

例として、下記内容での設定を示します。

・ VLAN モード :〔シングルタグ〕を選択

```
# admin vlan mode 2 singletag

#
```

手順6　IP インターフェース 2 番を有効にします。

```
# admin ip status 2 enabled

#
```

◆VLAN（VLAN ether）の設定

本装置の Ethernet ポートの VLAN 設定を行います。Ethernet ポートの VLAN 設定には CLI コンソールを使用します。

手順7　Ethernet ポートのタグなしフレーム許可設定を禁止に設定します。

```
# vlan ether untagframe deny

#
```

手順8　Ethernet ポートに VLAN-ID :「100」をタグなしで設定します。

```
# vlan ether set 100 untagged

#
```

手順9　Ethernet ポートの登録 VLAN 設定を有効に設定します。
※本設定実行後、telnet によるリモート接続は切断されます。

```
# vlan ether status enabled

#
```

◆IP アドレス設定

LTE/3G の設定は、Web コンソールを使用して設定します。WWW ブラウザに入力する IP アドレスは手順 3 で設定した IP アドレスを入力してください。

手順10 〔システム設定〕 → 〔監視インターフェース設定〕 → 〔IP アドレス設定〕を選択します。

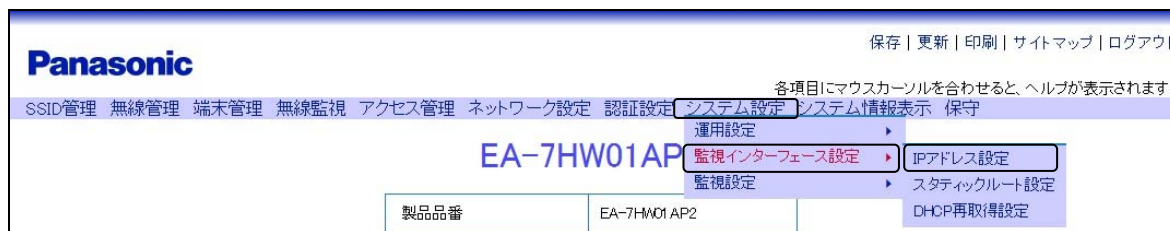



図3.3-1 メニュー（IP アドレス設定）

手順11 対象となる IP インターフェース 1 番の〔編集〕ボタンをクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守

IPアドレス設定

自装置のIPアドレスの設定を行います。
完全に独立したIPインターフェースが16個まで登録可能です。IPアドレスなどの設定値は重複登録が可能です。

IPアドレス設定一覧

IP-IF No. *1	状態	動作モード	IPアドレス	サブネットマスク	デフォルトゲートウェイ	VLANモード	
1	有効	Ethernet(固定)	192.168.0.3	255.255.255.0	192.168.0.1	タグなし	編集 再取得
2	有効	Ethernet(固定)	192.168.0.100	255.255.255.0	192.168.0.1	シングルタグ	編集 再取得
3	無効	Ethernet(自動)	---.---.---.---	---.---.---.---	---.---.---.---	タグなし	編集 再取得

図3.3-2 IP アドレス設定

手順 12 ～ 手順 13 は〔IP アドレス編集〕画面（図 3.3-3）より各種設定を行います。

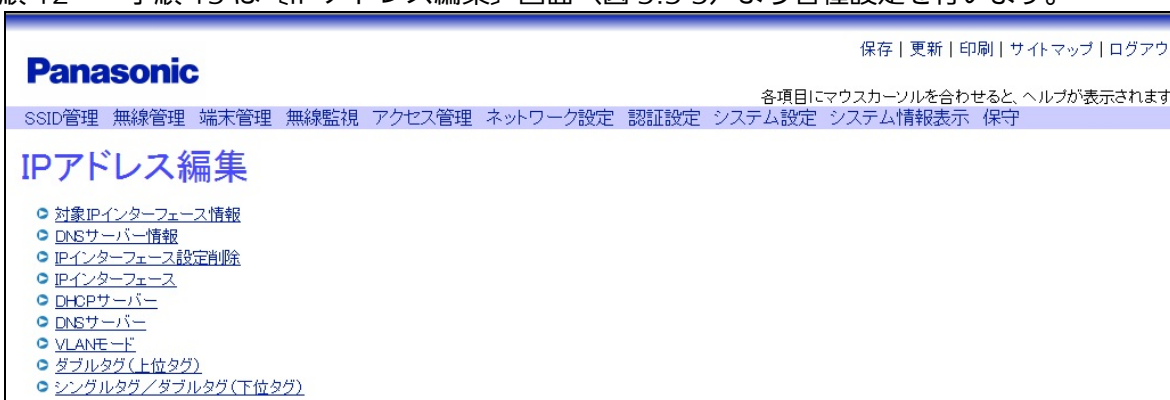



図3.3-3 IP アドレス編集

手順12　〔IP アドレス編集〕画面（図 3.3-3）の IP インターフェースをクリックし、IP インターフェース 1 番に対して下記設定を行います。

- インターフェースの〔有効〕を選択
- 動作モードの〔PPP〕を選択
- PPP 動作モードの〔LTE〕を選択

※PPP 動作モードの設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図3.3-4　 IP インターフェース

手順13　画面最下部の〔設定〕ボタンをクリックし、設定を反映させます。

◆LTE/3G 設定

手順14　〔ネットワーク設定〕　→　〔LTE/3G 設定〕　を選択します。

図3.3-5　 メニュー（LTE/3G 設定）

手順15　〔LTE/3G 設定〕をクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

LTE/3G設定

LTE/3G設定に関する詳細設定を行います。
LTE設定を使用する場合はIPアドレス編集画面にて動作モード「PPP」を選択後、PPP動作モードを「LTE」に変更してください。

- LTE/3G状態表示
- LTE/3G設定
- LTE/3G再接続制御
- LTE/3Gデバイスリセット

図3.3-6　 LTE/3G 設定

手順16　APN を入力します。
（APN はプロバイダから指定された値を設定してください。）

LTE/3G設定	
APN	(0～32文字)
LTE/3G自動再接続	○有効 ◉無効
LTE/3G自動再接続間隔	60 分 (10～1440)
LTE/3Gデバイス自動リセット	○有効 ◉無効
LTE/3Gデバイス自動リセット時刻 *1	3 時 (0～23)

図3.3-7　LTE/3G 設定（APN）

手順17　LTE/3G 設定下部の〔設定〕ボタンを押し、設定を反映させます。

◆PPP 設定

手順18　〔ネットワーク設定〕　→　〔PPP 設定〕　を選択します。

図3.3-8　メニュー（PPP 設定）

手順19　IP インターフェース選択の IP インターフェース番号に LTE/3G 接続する IP インターフェース番号を選択し、〔表示〕ボタンをクリックします。

図3.3-9　PPP 設定

手順20　PPP 設定をクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守
PPP設定
PPPに関する設定を行います。
IPインターフェース情報
PPP状態
PPP設定
IPインターフェース選択
IPインターフェース番号　一覧参照　1
表示

図3.3-10　　PPP 設定

手順21　PPP 設定にて下記設定を行います。

・　認証方式に〔PAP もしくは CHAP〕を選択
・　ログイン名にプロバイダから指定された値を入力
・　パスワードにプロバイダから指定された値を入力

※PPP 設定は、PPPoE と LTE で共通です。

図3.3-11　　PPP 設定

手順22　LTE/3G モジュールを USB ポートに接続します。

重要	■ LTE/3G 網を利用しての無線端末データ転送を行う場合、L2TP＋IPsec のようなインターネット VPN 接続設定も必要となります。LTE/3G 網を利用してのインターネット VPN 接続設定は「5.3　LTE/3G 接続を利用してのインターネット VPN 接続」を参照してください。 ■ LTE/3G モジュールを USB ポートに接続する際、延長ケーブルを使用する場合には、3m 以内の延長ケーブルを使用してください。

3.4　SSID の設定

本装置に異なる複数の SSID を設定し、各 SSID に異なる VLAN をマッピングさせることで、1 つのシステムで独立した複数のネットワーク接続を提供することができます。
SSID は最大 16 個まで本装置に多重できますので、仮想 AP が 16 台まで設定されることになります。本装置はデュアルバンド（2.4GHz／5GHz）の無線インターフェースを搭載しており、同じ SSID が仮想 AP の各無線インターフェースに設定されますので、ユーザーは無線 LAN 端末のインターフェースを意識することなく、本装置と接続し通信を行うことができます。

設定手順

◆SSID の生成
ここからは、Web コンソールを使用して設定します。

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

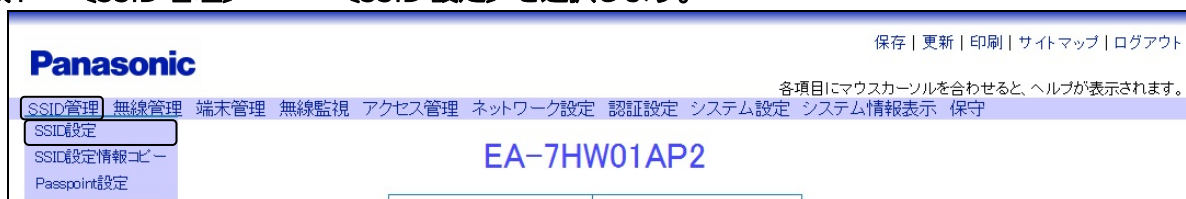



図3.4-1　メニュー（SSID 設定）

手順2　〔SSID 生成〕をクリックします。

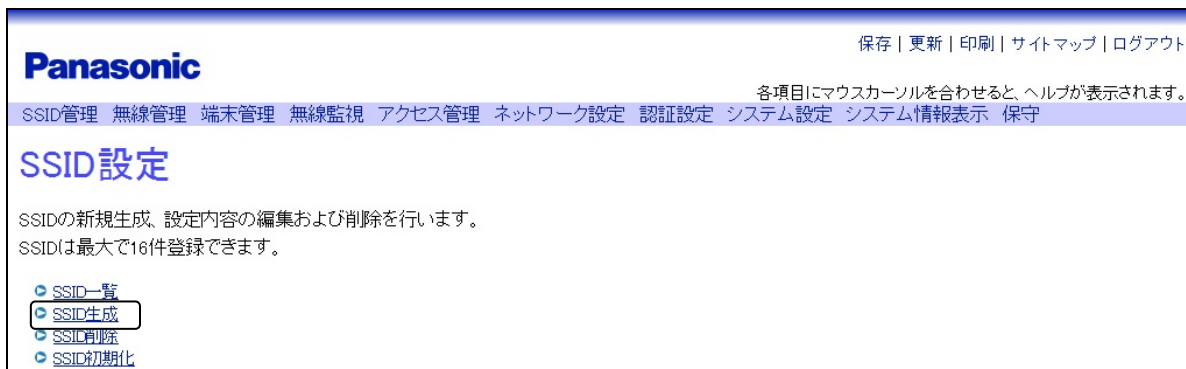



図3.4-2　SSID 設定

手順3　新たに作成するSSIDのプロファイル名（SSID 名）を指定します。

例として、SSID 番号 1 に営業部門用の SSID 名「SalesGroup」を生成します。

・ SSID 番号〔1〕を選択
・ SSID 名に「SalesGroup」を入力

上記操作後、〔生成〕ボタンをクリックします。

図3.4-3　SSID 生成

重要	■ ここで設定する SSID 名は、システム内で SSID を識別するために使用します。他の SSID の SSID 名と重複しないように設定してください。また、ビーコンに付与される SSID 値は、SSID 編集（後述）で使用します。

設定手順

◆SSID の設定

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

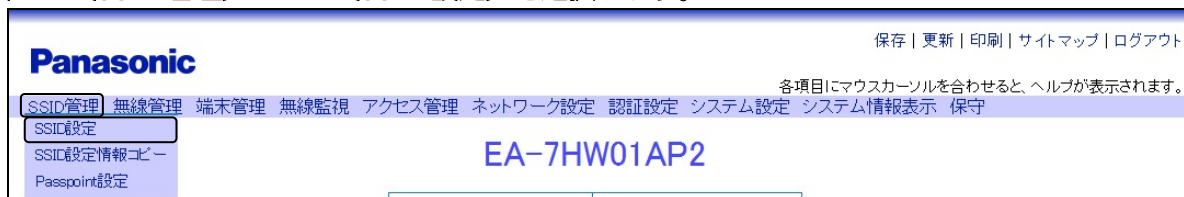



図3.4-4　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

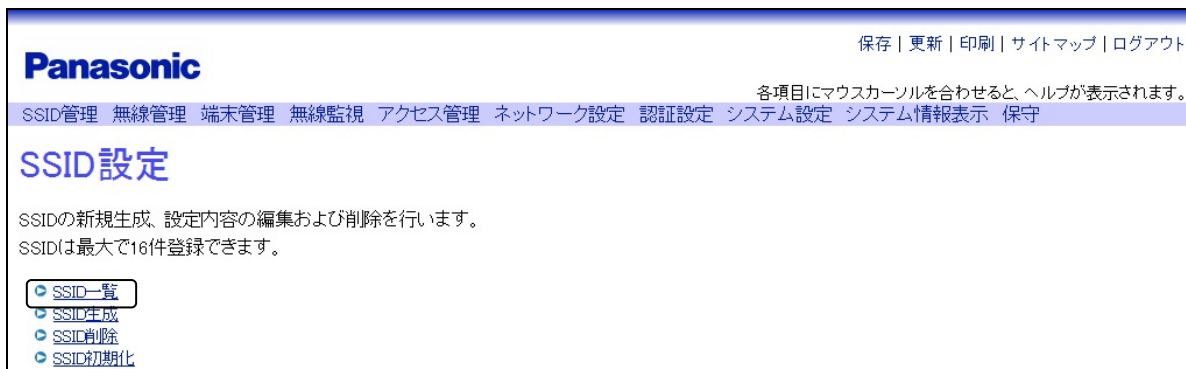



図3.4-5　SSID 設定

手順3　対象となる SSID の〔編集〕ボタンをクリックします。
例として、「SalesGroup」の編集を行います。

SSID番号	SSID名	SSID値（先頭の20文字を表示します）	VLANモード	SSID VLAN-ID	スイッチングモード設定	
1	SalesGroup		OFF	1	折り返しあり	編集

図3.4-6　SSID 一覧

〔SSID 編集〕画面が表示されます（図 3.4-7）。こちらより SSID の各種設定を行います。

図3.4-7　SSID 編集

手順4　〔SSID 情報〕をクリックし、SSID 値を設定します。

例として、SSID 名「SalesGroup」に対して SSID 値「SALES」を設定します。
ここで設定した SSID 値が ビーコン に付与されます。

図3.4-8　SSID 情報

手順5　〔SSID 編集〕画面（図 3.4-7）の〔利用する無線インターフェース〕をクリックし、利用する無線インターフェースを〔有効〕にします。

例として、2.4GHz 帯、5GHz 帯の両方を有効にします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
利用する無線インターフェース

2.4GHz帯	◉有効 ○無効
5.0GHz帯	◉有効 ○無効

図3.4-9　利用する無線インターフェース

手順6　〔SSID 編集〕画面（図 3.4-7）の〔無線モード〕をクリックし、2.4GHz 帯と 5GHz 帯の無線モードを選択します。

例として、下記内容での設定を示します。

- 2.4GHz 帯：〔11bgn〕を選択
- 5GHz 帯：〔11an〕を選択

図3.4-10　無線モード

手順7　〔SSID 編集〕画面（図 3.4-7）の〔IEEE802.11 設定〕をクリックし、IEEE802.11 に 関する設定を行います。

802.11 認証アルゴリズムに関して、詳細は「4.2　セキュリティー設定」をご参照ください。

例として、下記内容での設定を示します。

- Any 接続拒否：〔しない〕を選択（無線 LAN 端末から本装置を検索可とします。）
- SSID の隠蔽：〔しない〕を選択（ビーコンに SSID 名を載せます。）

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

IEEE802.11設定

Any接続拒否	する　しない
SSIDの隠蔽	する　しない
802.11認証アルゴリズム	open　shared　両方

図3.4-11　IEEE802.11 設定

手順8　〔SSID 編集〕画面（図 3.4-7）の〔VLAN モード〕をクリックし、VLAN モードを選択します。

〔SSID〕を選択した場合は、SSID ごとに VLAN を分離します。

〔SSID　&　User〕、〔User〕については、「4.2.4 ユーザー認証」をご参照ください。

図3.4-12　VLAN モード

手順9　〔SSID 編集〕画面（図 3.4-7）の〔SSID VLAN〕をクリックし、VLAN-ID を設定します。

図3.4-13　SSID VLAN

手順 8 にて「User」、または「SSID & User」を選択した場合は、〔User VLAN〕の設定を行います。（図 3.4-14）

図3.4-14　User VLAN

手順10　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

■以下の編集項目については、各種機能設定を参照ください。

・セキュリティー(EAP 認証)
・IEEE802.1X 認証
・暗号鍵更新設定
・MAC 認証
・認証動作設定
・Authentication・Accounting
・無線プロビジョニングサービス
・連続接続制限

4.2　セキュリティー設定

・代理 ARP 応答
・通信端末数による端末接続制御

4.6　VoIP 利用時の各種設定

・QoS

4.1　QoS

・IGMP スヌーピング

4.7　サービス品質向上機能

・Web 認証
・Web 認証 AP 間連携

4.8　Web 認証

・アグリゲーション
・LDPC 符号化

4.9　その他の機能

3.5　SSID 多重設定

2.4GHz 帯と 5GHz 帯の無線インターフェースにおける、SSID ごとの送信制御やデータレートの設定を行います。

設定手順

◆SSID 多重での SSID 動作設定

SSID の生成と設定は前節にて実施済みとします。

手順1　〔無線管理〕　→　〔SSID 多重設定〕を選択します。

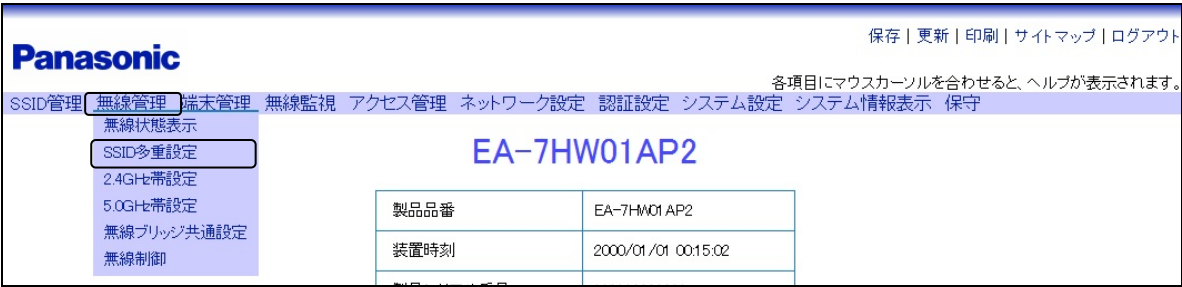



図3.5-1　メニュー（SSID 多重設定）

手順2　対象となる SSID の〔編集〕ボタンをクリックします。

例として、登録番号：1 の編集を行います。

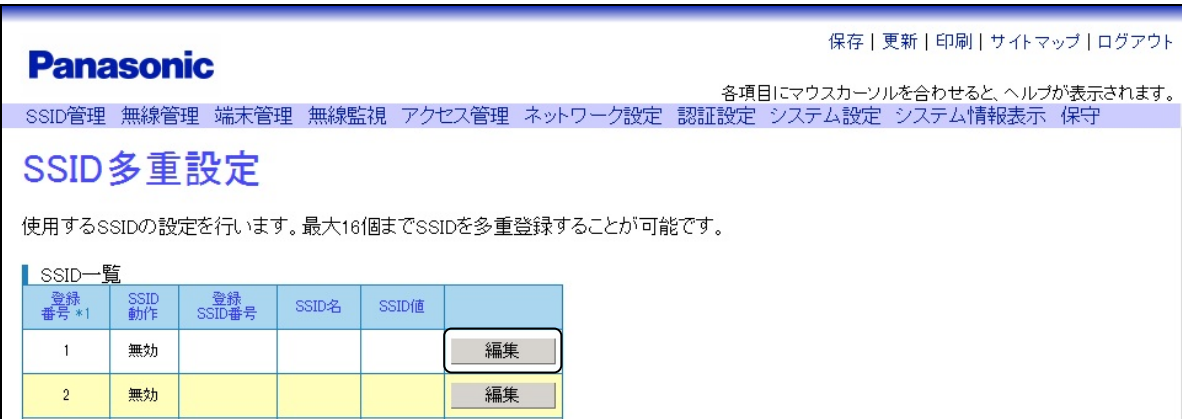



図3.5-2　SSID 多重設定

手順3　〔SSID 登録〕をクリックします。

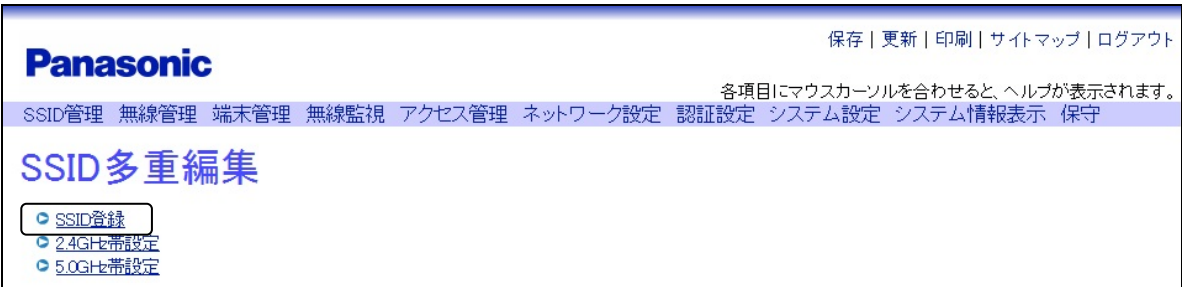



図3.5-3　SSID 多重編集

手順4　SSID 登録を行います。

例として、下記内容での設定を示します。

・ SSID 動作：〔有効〕を選択
・ 登録 SSID 番号：〔1〕を選択（手順 2 で選択した登録番号に紐付けする SSID 番号を選択。）

図3.5-4　SSID 登録

手順5　〔SSID 多重編集〕画面（図 3.5-3）の〔2.4GHz 帯設定〕、または〔5.0GHz 帯設定〕をクリックし、マルチキャスト・ブロードキャストの送信制御、および各種データレート設定を行います。

例として、2.4GHz 帯設定を選択し、設定を行います。

・ ブロードキャスト制御：〔送信遮断を行わない〕を選択
・ マルチキャスト制御：　〔送信遮断を行わない〕を選択
・ 制御モード：〔自動〕を選択
・ 最小値（レガシー）：〔1M〕を選択
・ 最大値（レガシー）：〔54M〕を選択
・ 最小値（11n）：〔15M〕を選択
・ 最大値（11n）：〔450M〕を選択
・ ブロードキャストレート制御：〔無効〕を選択
・ マルチキャストレート制御：〔無効〕を選択
・ ビーコンレート制御：〔無効〕を選択

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

2.4GHz帯設定

送信制御	ブロードキャスト制御	○送信遮断を行う ◉送信遮断を行わない
	マルチキャスト制御	○送信遮断を行う ◉送信遮断を行わない
データレート 一覧参照 *3	制御モード	○固定 ◉自動
	最小値(レガシー) *2	1M
	最大値(レガシー) *2	54M
	最小値(11n) *3	15M
	最大値(11n) *3	450M
	ブロードキャストレート制御	○有効 ◉無効
	ブロードキャストレート *4	24M
	マルチキャストレート制御	○有効 ◉無効
	マルチキャストレート *4	24M
	ビーコンレート制御	○有効 ◉無効
	ビーコンレート *4	24M
帯域比率		1 (1～10)

図3.5-5　2.4GHz 帯設定（SSID 多重設定）

〔5.0GHz 帯設定〕も〔2.4GHz 帯設定〕の画面（図 3.5-5） と同様です。

レガシーレートの大きさは、
11b（1M<2M<5.5M<11M）<11g（6M<9M<12M<18M<24M<36M<48M<54M）
の順になります。
また、ブロードキャスト／マルチキャスト／ビーコンのレート設定を使用する場合は、それぞれの
レート制御モードを「有効」に設定してください。

帯域比率について、詳細は「4.1　QoS」をご参照ください。
11n レートの設定は、周波数帯域幅 40MHz、GI=400ns を基準に行います。
実際に設定される送信レートは、下表の通り、周波数帯域幅・GI（ガードインターバル）と
設定する最高送信レートや最低送信レートによって、選択されるレートが変わります。
設定する送信レートは、下表の設定レートの列を参照してください。

例）周波数帯域幅：20MHz、最高送信レート：450M を指定した場合は、最高送信
　　レートとして 216.7M が選択されます。（GI：400ns の場合）

表3.5-1　　レート制御

MCS *	変調方式	符号化率	空間多重数	データレート				設定レート
				20MHz		40MHz		
				GI=800ns	GI=400ns	GI=800ns	GI=400ns	
0	BPSK	1/2	1	6.5	7.2	13.5	15.0	15.0
1	QPSK	1/2	1	13.0	14.4	27.0	30.0	30.0
2	QPSK	3/4	1	19.5	21.7	40.5	45.0	45.0
3	16QAM	1/2	1	26.0	28.9	54.0	60.0	60.0
4	16QAM	3/4	1	39.0	43.3	81.0	90.0	90.0
5	64QAM	2/3	1	52.0	57.8	108.0	120.0	120.0
6	64QAM	3/4	1	58.5	65.0	121.5	135.0	135.0
7	64QAM	5/6	1	65.0	72.2	135.0	150.0	150.0
8	BPSK	1/2	2	13.0	14.4	27.0	30.0	30.0
9	QPSK	1/2	2	26.0	28.9	54.0	60.0	60.0
10	QPSK	3/4	2	39.0	43.3	81.0	90.0	90.0
11	16QAM	1/2	2	52.0	57.8	108.0	120.0	120.0
12	16QAM	3/4	2	78.0	86.7	162.0	180.0	180.0
13	64QAM	2/3	2	104.0	115.6	216.0	240.0	240.0
14	64QAM	3/4	2	117.0	130.0	243.0	270.0	270.0
15	64QAM	5/6	2	130.0	144.4	270.0	300.0	300.0
16	BPSK	1/2	3	19.5	21.7	40.5	45.0	45.0
17	QPSK	1/2	3	39.0	43.3	81.0	90.0	90.0
18	QPSK	3/4	3	58.5	65.0	121.5	135.0	135.0
19	16QAM	1/2	3	78.0	86.7	162.0	180.0	180.0
20	16QAM	3/4	3	117.0	130.0	243.0	270.0	270.0
21	64QAM	2/3	3	156.0	173.3	324.0	360.0	360.0
22	64QAM	3/4	3	175.5	195.0	364.0	405.0	405.0
23	64QAM	5/6	3	195.0	216.7	405.0	450.0	450.0

＊MCS：Modulation and Coding Scheme

手順6　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

3.6　各無線インターフェースの設定

2.4GHz 帯・5GHz 帯それぞれの周波数帯における、詳細設定を行います。

設定手順

◆無線インターフェースの設定

手順1　〔無線管理〕　→　〔2.4GHz 帯設定〕、または〔5.0GHz 帯設定〕を選択します。

例として、2.4GHz 帯設定を選択します。

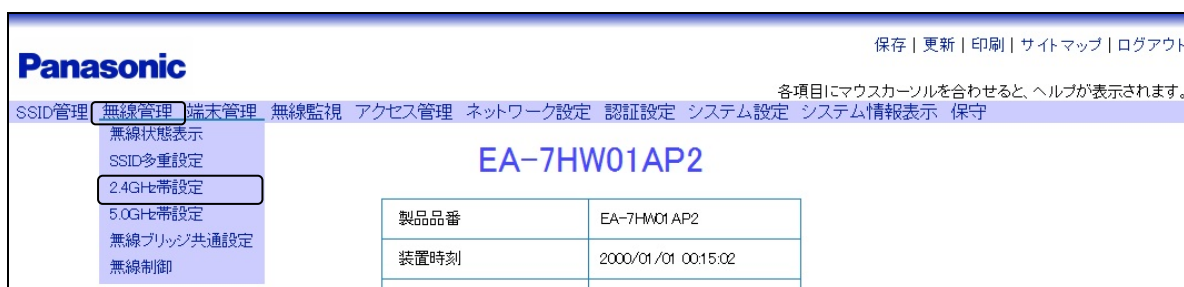



図3.6-1　メニュー（2.4GHz 帯設定）

手順 2 ～ 手順 4 は〔2.4GHz 帯設定〕画面（図 3.6-2）より各種設定を行います。

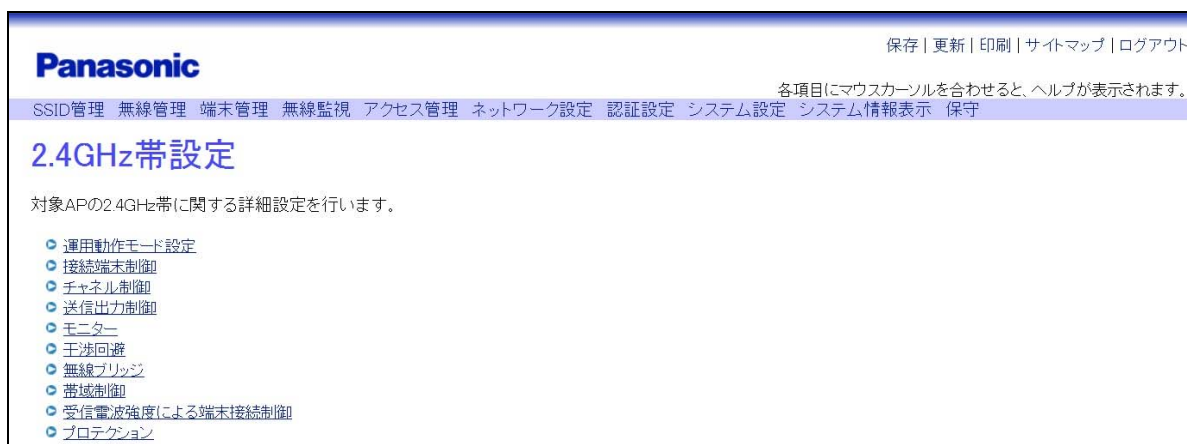



図3.6-2　2.4GHz 帯設定

手順2　〔2.4GHz 設定〕画面（図 3.6-2）で〔運用動作モード〕をクリックします。

例として、下記内容での設定を示します。

・　無線インターフェース：〔有効〕を選択
・　動作モード：〔通常運用〕を選択

※動作モードの設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

運用動作モード設定

項目	設定
無線インターフェース	◉有効 ○無効
動作モード (注1)	◉通常運用 ○無線モニター
ビーコン間隔 *1	100 ミリ秒 (20～1000)
DTIM間隔	1 (1～255)
TKIP *2 (注1)	○有効 ◉無効

図3.6-3　運用動作モード設定

手順3　〔2.4GHz 設定〕画面（図 3.6-2）で〔チャネル制御〕をクリックします。

例として、下記内容での設定を示します。

・　チャネル制御モード：〔自動〕を選択

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

チャネル制御

項目		設定
チャネル制御モード		○固定 ◉自動
チャネル番号 *3		1
選択可能チャネル *4	1ch	◉選択可能にする ○選択可能にしない
	2ch	◉選択可能にする ○選択可能にしない
	3ch	◉選択可能にする ○選択可能にしない
	4ch	◉選択可能にする ○選択可能にしない
	5ch	◉選択可能にする ○選択可能にしない
	6ch	◉選択可能にする ○選択可能にしない
	7ch	◉選択可能にする ○選択可能にしない
	8ch	◉選択可能にする ○選択可能にしない
	9ch	◉選択可能にする ○選択可能にしない
	10ch	◉選択可能にする ○選択可能にしない
	11ch	◉選択可能にする ○選択可能にしない
	12ch	◉選択可能にする ○選択可能にしない
	13ch	◉選択可能にする ○選択可能にしない
周波数帯域幅		◉20MHz ○20MHz/40MHz
40MHz復旧監視機能 *5		○有効 ◉無効
40MHz復旧監視間隔		30 分 (1～1440)

図3.6-4　チャネル制御（2.4GHz）

手順4　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

5GHz 帯設定時は、図 3.6-5　の画面が表示されます。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

チャネル制御

項目		設定
チャネル制御モード		○固定 ⦿自動
チャネル番号 *3 *4		36
選択可能チャネル *5	36ch	⦿選択可能にする ○選択可能にしない
	40ch	⦿選択可能にする ○選択可能にしない
	44ch	⦿選択可能にする ○選択可能にしない
	48ch	⦿選択可能にする ○選択可能にしない
	52ch	⦿選択可能にする ○選択可能にしない
	56ch	⦿選択可能にする ○選択可能にしない
	60ch	⦿選択可能にする ○選択可能にしない
	64ch	⦿選択可能にする ○選択可能にしない
	100ch	⦿選択可能にする ○選択可能にしない
	104ch	⦿選択可能にする ○選択可能にしない
	108ch	⦿選択可能にする ○選択可能にしない
	112ch	⦿選択可能にする ○選択可能にしない
	116ch	⦿選択可能にする ○選択可能にしない
	120ch	⦿選択可能にする ○選択可能にしない
	124ch	⦿選択可能にする ○選択可能にしない
	128ch	⦿選択可能にする ○選択可能にしない
	132ch	⦿選択可能にする ○選択可能にしない
	136ch	⦿選択可能にする ○選択可能にしない
	140ch	⦿選択可能にする ○選択可能にしない
周波数帯域幅		⦿20MHz ○20MHz/40MHz
40MHz復旧監視機能 *6		○有効 ⦿無効
40MHz復旧監視間隔		30 分 (1～1440)

図3.6-5　チャネル制御（5GHz）

重要	■ W52（36ch～48ch）、W53（52ch～64ch）は、電波法により屋内使用限定です。屋外使用の場合、チャネル番号設定には、「36ch～64ch」を選択しないでください。また、チャネル制御モードが自動設定の場合、選択可能チャネル設定については、「36ch～64ch」は、「選択可能にしない」を選択してください。 ■ 5GHz 帯でのみ 40MHz 運用が可能なため、2.4GHz 設定では周波数帯域幅は 20MHz、40MHz 復旧監視機能は無効のみ設定可能です。

その他、周波数帯における詳細設定の変更を行う場合は、以降の設定を行います。

◆接続端末制御

対象無線インターフェースの最大接続可能端末数を設定します。
※この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図3.6-6　接続端末制御

◆送信出力制御

本装置の出力レベルを選択します。

図3.6-7　送信出力制御

◆モニター

全チャネルスキャンの有効／無効を設定します。
有効を選択した場合は、モニター間隔を設定します。
※モニター：〔有効〕を設定した場合、パケットロスが発生したり、接続した端末が切断される可能性があります。

図3.6-8　モニター

◆干渉回避

チャネル制御を自動で行っている際、干渉により使用可能なチャネルが存在しなかった場合の最終動作を選択します。

図3.6-9　干渉回避

◆**無線ブリッジ**

無線ブリッジにおける各設定を行います。（詳細は、4.5 無線ブリッジを参照してください。）

※〔MAC ブリッジ動作許可設定〕の変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図3.6-10　　無線ブリッジ

◆**帯域制御**

本装置と無線 LAN 端末間でのパケットの帯域制御方法を設定します。

※この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。なお、本機能の詳細は「4.1　QoS」をご参照ください。

図3.6-11　　帯域制御

◆受信電波強度による端末接続制御

接続している端末台数が設定した閾値に達した場合、電波の弱い端末の接続要求を拒否する機能の設定を行います。

図3.6-12　受信電波強度による端末接続制御

◆プロテクション

11b 端末と 11g 端末が同時に接続された場合の干渉保護動作の判定方法（IEEE802.11g プロテクション動作）と 11n 未対応端末に対する干渉保護動作（HT プロテクション）の設定を行います。

図3.6-13　プロテクション（2.4GHz）

図3.6-14　プロテクション（5GHz）

第４章　各種機能設定

本装置の各種機能について、説明します。

4.1 QoS

本装置の QoS 機能（優先制御・帯域制御）設定について説明します。

4.1.1 SSIDごとの帯域制限

帯域制御設定とは、本装置が提供する QoS 機能の 1 つであり、無線 LAN アクセスポイントに多重している SSID ごとに 10 段階の比率を設定することで、下りデータのトラフィック輻輳時に当該 SSID が使用できる帯域幅に差をつけることができます。
ここでは、下り無線区間輻輳時に SSID1 と SSID2 のトラフィックが利用できる帯域を割り当てる方法を紹介します。
以下の例では、下り無線区間輻輳時には、SSID1：SSID2＝5：1 の帯域を割り当てます。
この帯域制御動作は、無線区間の輻輳時に機能し、輻輳していない状態では必要な帯域を使用することができ、空き帯域を有効に利用できます。同じ SSID を使用する端末の帯域比率は均等になります。

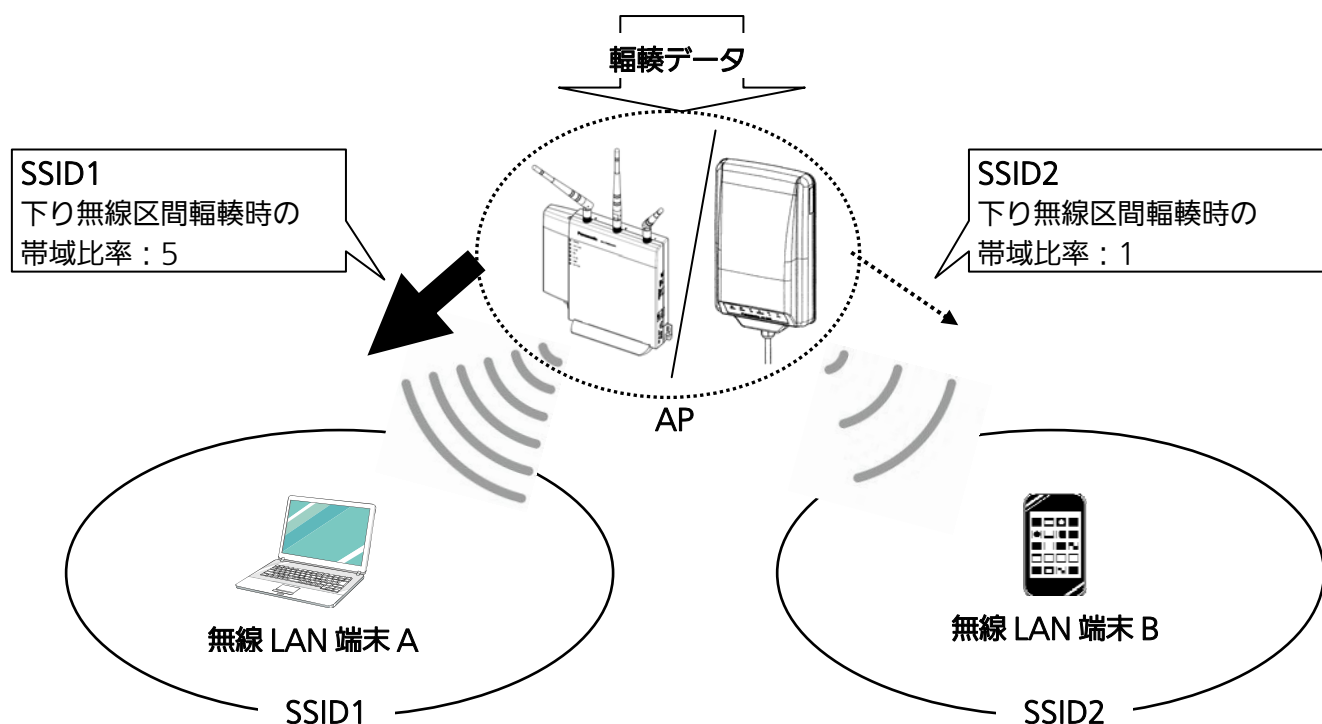



図4.1-1　帯域制御動作

設定手順

◆帯域制御の設定

ここでは 2.4GHz 帯の設定を行なうものとします。

手順1　〔無線管理〕　→　〔2.4GHz 帯設定〕を選択します。

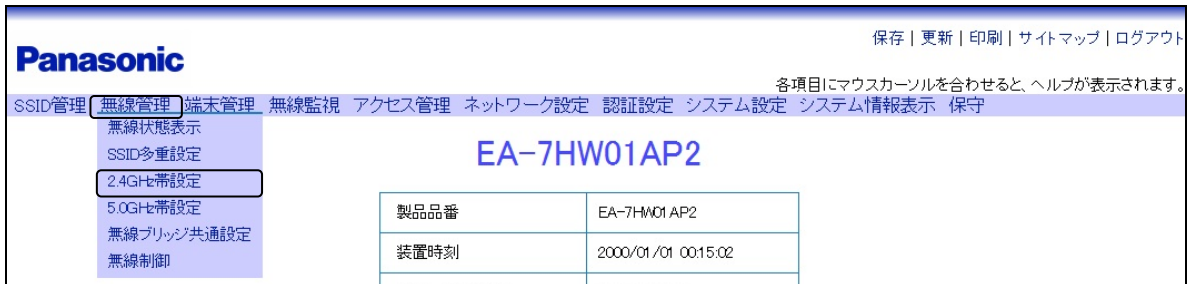



図4.1-2　メニュー（2.4GHz 帯設定）

手順2　〔帯域制御〕をクリックします。

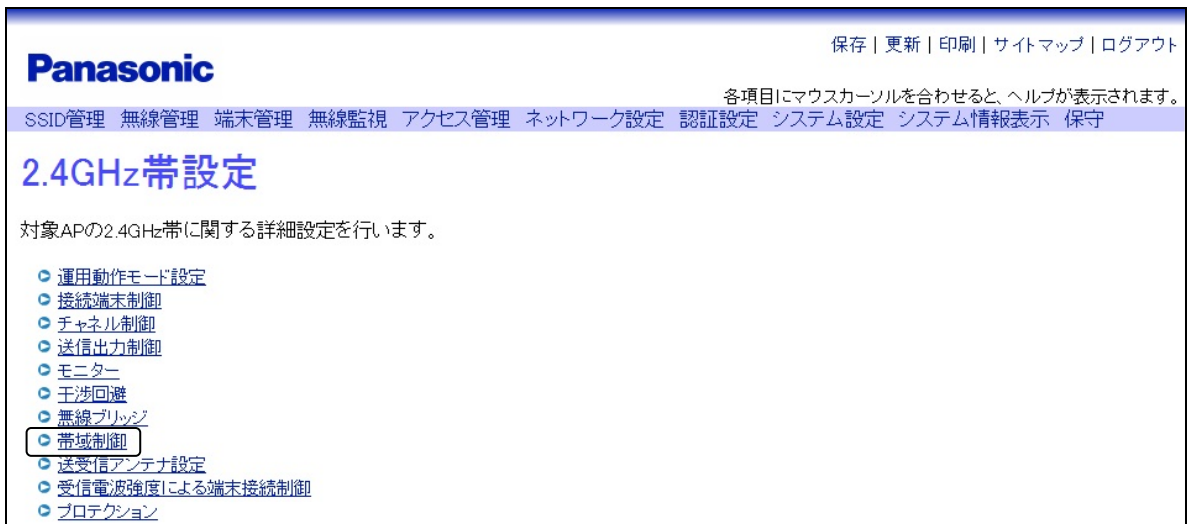



図4.1-3　2.4GHz 帯設定

手順3　〔有効〕を選択します。

※この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図4.1-4　帯域制御

手順4　画面最下部〔設定〕ボタンを押し、設定を反映させせます。

設定手順

◆帯域比率の設定

手順1　〔無線管理〕　→　〔SSID 多重設定〕を選択します。

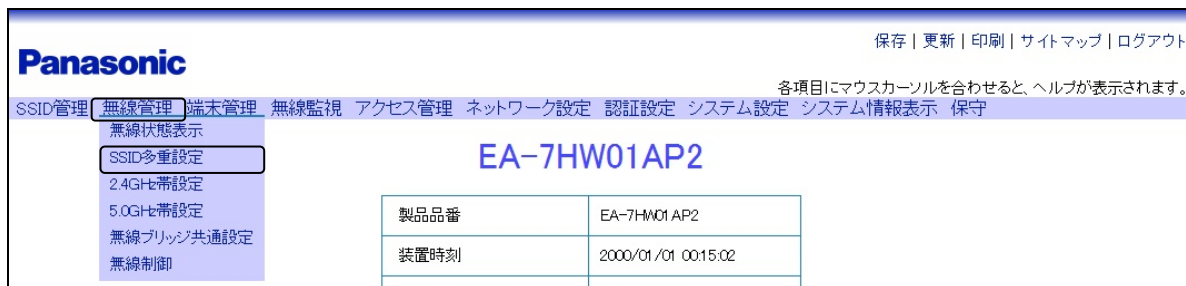



図4.1-5　メニュー（SSID 多重設定）

手順2　対象となる SSID の〔編集〕ボタンをクリックします。

例として SSID1 を指定します。

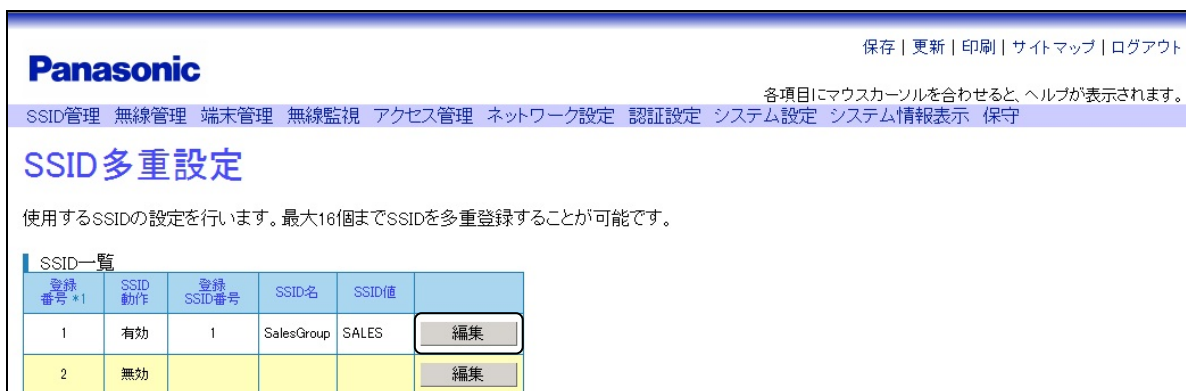



図4.1-6　SSID 多重設定

手順3　〔2.4GHz 帯設定〕をクリックします。

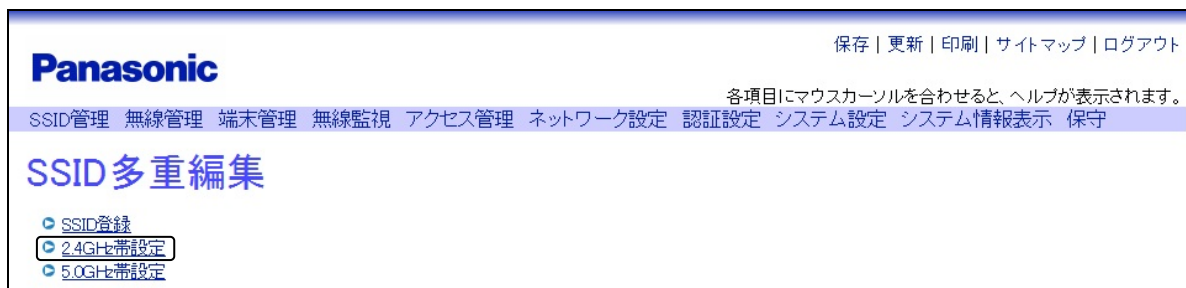



図4.1-7　SSID 多重編集

手順4　「帯域比率」を（1～10）の任意の値で設定します。
　例として「1」を入力します。

図4.1-8　2.4GHz 帯設定（帯域比率)

手順5　画面最下部〔設定〕ボタンを押し、設定を反映させます。

※必要に応じて、同じ無線インターフェース番号に登録している他の SSID に対しても帯域を設定
　してください。

4.1.2　フローごとの優先制御

優先制御設定とは、本装置が提供する QoS 機能の 1 つであり、SSID 内を流れるデータフレームの条件を定義し、その条件に一致するデータフレームを優先することができます。優先制御は、優先設定・CoS 値設定・TOS 値設定の 3 つの設定があり、無線 LAN 接続・無線ブリッジ接続それぞれに設定できます。
条件には、ブリッジ条件、または IP 条件を用いることができます。

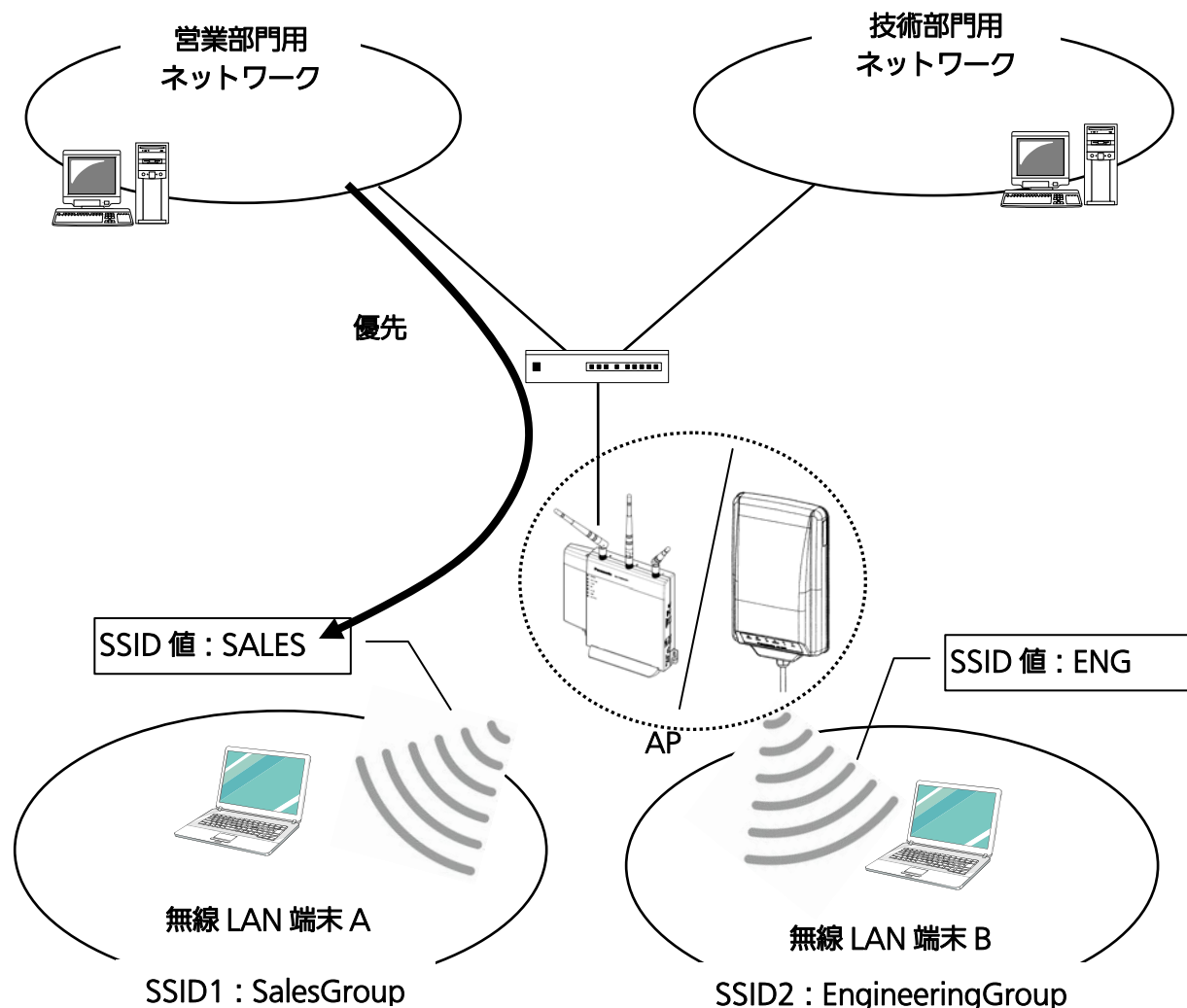



図4.1-9　優先制御例

■優先制御の動作モード

優先制御の動作モードには、WMM（WMM® （Wi-Fi Multimedia ™ ）に沿った QoS 制御）と WRR（重みつきラウンドロビン転送)、OFF（QoS 制御をしない）の 3 種類があります。WMM モードでは、WMM 対応無線 LAN 端末との間で上り下り方向無線データの優先制御を行うことができます。WRR モードでは、WMM 非対応無線 LAN 端末に対し、下り方向無線データの優先制御を行うことができます。

表4.1-1　動作モード一覧

モード	説明	備考
WMM	WMM 対応無線 LAN 端末と上り下り両方向の 無線データに対する優先制御を行います。	
WRR	下り方向の無線データに対する優先制御を行います。	・WPA/IEEE802.11i･WPA2 の認証モード時は設定できません。 ・SSID の無線モードが 11n 対応モード時は､WMM 固定で動作します。
OFF	QoS 制御を行わない。	・SSID の無線モードが 11n 対応モード時は､WMM 固定で動作します。

■優先制御の概要

WRR、WMM を選択した場合は、データフレームに優先制御の条件設定を行います。条件にはブリッジ条件と IP 条件があり、それぞれ送信元 MAC アドレスや送信先 MAC アドレス、送信元 IP アドレスや送信先 IP アドレスなどを条件として設定できます。ただし、WMM ではデータフレーム内の DSCP／CoS 値により自動的に下り方向無線データの優先度が割り当てられます。

表4.1-2　アクセスコントロールプライオリティの割当

設定項目	単位	値および意味	最大登録可能数
ブリッジ条件	装置	送信元 MAC アドレス 送信先 MAC アドレス イーサタイプ VLAN CoS	512
IP 条件	装置	送信元 IP アドレス 送信元 IP マスク値 送信先 IP アドレス 送信先 IP マスク値 TOS 値 プロトコル番号 送信元ポート 送信先ポート	512
ブリッジ条件のアクセスカテゴリープライオリティ	SSID	0～3：プライオリティ	32
IP 条件のアクセスカテゴリープライオリティ	SSID	0～3：プライオリティ	32

条件設定の詳細は、「4.4　フィルタリング」を参照してください。

設定手順

◆優先制御の設定

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

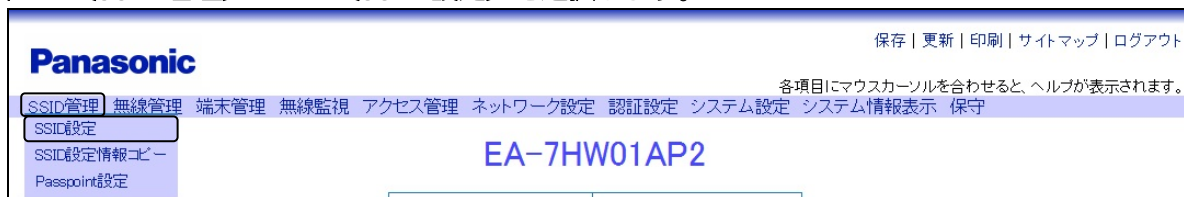



図4.1-10　メニュー（SSID 設定）

手順2　対象となる SSID の〔編集〕ボタンをクリックします。

図4.1-11　SSID 一覧

手順3　〔QoS〕をクリックします。

図4.1-12　SSID 編集（QoS）

手順4　〔WMM規格に沿ったQoS制御〕を選択します。

QoS動作 *12	◎重みつきラウンドロビン転送 ◉WMM規格に沿ったQoS制御 ◎QoS制御をしない
TSPECアドミッション受付(音声:AC_VO)	◎有効 ◉無効
TSPECアドミッション受付(映像:AC_VI)	◎有効 ◉無効
U-APSD機能	◎有効 ◉無効

図4.1-13　QoS

手順5　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

※VoIP利用時に自動的に優先割り当てを行う簡易設定があります。「4.6.3　VoIP /Video自動優先割り当て」を参照してください。

4.2 セキュリティー設定

本装置は、無線 LAN サービスにおける認証・暗号化によるセキュリティー機能を備えています。認証および暗号化は、SSID ごとに設定できます。

4.2.1 認証と暗号化

本装置では、無線 LAN 環境のセキュリティーを確保するために、セキュリティー機能（認証および暗号化）を備えています。SSID ごとに異なる暗号化を設定することはもちろん、同一 SSID 上に複数の暗号化方式を混在させることも可能です。これによって、ノート PC や VoIP 電話など、多彩な通信機器が存在する現在のオフィス環境のセキュリティーにも対応できます。
本項では、本装置に備えられている認証方式および暗号化方式の概要を紹介します。

■ 認証方式

認証とは無線 LAN アクセスポイント を経由してネットワークに接続しようとするユーザーのアクセス権を照合するための処理であり、無線 LAN のセキュリティー確保には不可欠な機能です。
本装置が対応している認証方式には以下の 4 種類があります。

IEEE802.11 Authentication

IEEE802.11 標準が定める認証方式で、無線 LAN の接続要求時に行われます。認証方式には、open、shared、both（open と shared の両方をサポート）があります。他の認証方式との併用、または固定 WEP 以外の暗号化方式を利用する場合は、open を選択してください。

IEEE802.1X

IEEE802.1X 規格で定められた Authentication サーバーを使用する認証方式です。IEEE802.1X での認証は無線クライアントと認証サーバーで行われます。そして、認証後、無線クライアントには認証サーバーが作成した鍵が安全に配送される（動的 WEP）ため、より安全な接続が確保されます。
なお、IEEE802.1X の認証サーバーによる認証方式は、WPA や IEEE802.11i/WPA2 といった認証方式の中でも利用できます。

WPA

WPA は、「Wi-Fi Alliance」という米国の業界団体が定めた暗号化方式規格で、その中で認証方式も規定しています。Wi-Fi Alliance は、IEEE802.11i 標準策定前に、WEP の脆弱性を補った暗号方式である TKIP（Temporal Key Integrity Protocol）の仕様を切り出し、WPA として公開しました。
WPA が対応する認証方式には、PSK（事前共通鍵認証）と IEEE802.1X があります。

IEEE802.11i/WPA2

IEEE802.11i は、無線 LAN におけるセキュリティー標準を定める規格であり、先に WPA として切り出された仕様に、最新の暗号化形式である AES への対応を付け加えたものとなっています。
一方、WPA2 とは、Wi-Fi Alliance が公開した WPA の改良規格であり、IEEE802.11i に準拠しています。IEEE802.11i/WPA2 が対応する認証方式には、PSK（事前共通鍵認証）と IEEE802.1X があります。

■ 暗号化方式

無線 LAN の場合、AP の電波を誰でも受信できてしまいます。傍受を防ぎ、安全な通信を確保するためには、送受信されるデータを暗号化する必要があります。
本装置が対応している暗号化方式には以下の 3 種類があります。

WEP

RC4 というアルゴリズムに従った暗号化方式です。無線 LAN 端末と無線 LAN アクセスポイントに、固定的に WEP キーと呼ばれる暗号鍵を割り当てておく固定 WEP と、Authentication サーバーでの認証後、サーバーからダイナミックに WEP キーを割り当てる動的 WEP の 2 方式があります。
固定 WEP は解読されやすく、非常に脆弱です。動的 WEP は、固定 WEP に比べてセキュリティーは格段にアップしますが、動的 WEP を利用するためには Authentication サーバーの設定が必要となります。

TKIP

WEP の暗号化アルゴリズムをベースとして、その脆弱性を補うために改良・強化された暗号化方式です。

CCMP

次世代暗号化標準（AES）を元にした、WEP や TKIP とはまったく別の強固な暗号化アルゴリズムを採用した暗号化方式です。

4.2.2　認証方式と暗号化方式の組み合わせ

セキュリティーを設定する場合、認証方式と暗号化方式の両方を指定する必要があります。

■認証・暗号化の設定における共通操作

操作手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

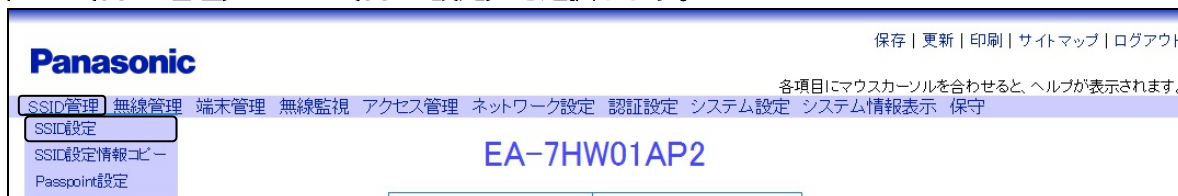



図4.2-1　メニュー（SSID 設定）

手順2　対象となる SSID の〔編集〕ボタンをクリックします。

図4.2-2　SSID 一覧

以降の設定は、SSID 編集画面（図 4.2-3）より行います。

図4.2-3　SSID 編集

■IEEE802.11 設定

設定手順

手順1　〔SSID 編集〕画面（図 4.2-3）の〔IEEE802.11 設定〕をクリックします。

手順2　802.11 認証アルゴリズムの設定を行います。

固定 WEP 以外の暗号化方式を使用する場合は、必ず〔open〕を選択してください。
固定 WEP を使用する場合は、〔open〕、〔shared〕、〔両方〕のどれを選択してもかまいません。

Panasonic
保存 | 更新 | 印刷 | サイトマップ | ログアウト
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
IEEE802.11設定

Any接続拒否	○する ◉しない
SSIDの隠蔽	○する ◉しない
802.11認証アルゴリズム	◉open ○shared ○両方

図4.2-4　IEEE802.11 設定

手順3　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

■固定 WEP

暗号化方式として、固定 WEP を使用する場合は、以下の設定を行ってください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-3）の〔セキュリティー（共通）〕をクリックします。

手順2　固定 WEP に関する設定を行います。

例として、下記内容での設定を示します。

- 固定 WEP〔有効〕を選択
- WEP キー〔WEP40〕または〔WEP104〕を選択
- キー入力〔ASCII〕を選択し、キー値に「A1234」を入力

Panasonic
保存 | 更新 | 印刷 | サイトマップ | ログアウト
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
セキュリティー(共通)

固定WEP	◉有効 ○無効
動的WEP	○有効 ◉無効
WEPキー *4	◉WEP40 ○WEP104 ◉ASCII ○HEX A1234 ☑ 入力確認

図4.2-5　セキュリティー（共通）固定 WEP 選択

表4.2-1　動作モード一覧表

	鍵長	HEX	ASCII
WEP40	40bit	10 桁	5 文字
WEP104	104bit	26 桁	13 文字

手順3　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

■動的 WEP
暗号化方式として、動的 WEP を使用する場合は、以下の設定を行ってください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-6）の〔セキュリティー（共通）〕をクリックします。
手順2　動的 WEP に関する設定を行います。
例として、下記内容での設定を示します。
- 動的 WEP 〔有効〕を選択
- WEP キー〔WEP40〕を選択

動的 WEP の場合、WEP キーの ASCII/HEX およびキーの設定は無視されます。
Authentication サーバーの設定については「4.2.3 Authentication サーバーを利用した IEEE802.1X 認証」を参照ください。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
セキュリティー(共通)

項目	設定
固定WEP	○有効 ◉無効
動的WEP	◉有効 ○無効
WEPキー *4	◉WEP40 ○WEP104
	◉ASCII ○HEX
	●●●●●●●●●●●●●
	□ 入力確認
WPA	○有効 ◉無効
WPA2	○有効 ◉無効
WPA/WPA2認証方法	◉802.1X ○PSK
TKIP *5	○有効 ◉無効
AES	◉有効 ○無効
PSK *6	◉HEX ○パスフレーズ
	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
	□ 入力確認

図4.2-6　セキュリティー（共通）動的 WEP 選択

手順3　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

■WPA と TKIP

認証方式として WPA を選択し、暗号化方式として TKIP を PSK（Authentication サーバーを使用しない）で利用する場合は、以下を設定してください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-6）の〔セキュリティー（共通)〕をクリックします。

手順2　WPA と TKIP に関する設定を行います。

例として、下記内容での設定を示します。

- WPA 〔有効〕を選択
- WPA/WPA2 認証方法〔PSK〕を選択
- TKIP 〔有効〕を選択

TKIP 有効の場合、各無線インターフェース設定画面の〔運用動作モード設定〕で、TKIP の〔有効〕を選択してください。

※この設定変更では、設定反映後の保存とリセットが必要となります。

- PSK〔パスフレーズ〕を選択し、暗号キーを入力

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

セキュリティー（共通）

固定WEP	有効 / 無効
動的WEP	有効 / 無効
WEPキー *4	WEP40 / WEP104 ASCII / HEX 入力確認
WPA	有効 / 無効
WPA2	有効 / 無効
WPA/WPA2認証方法	802.1X / PSK
TKIP *5	有効 / 無効
AES	有効 / 無効
PSK *6	HEX / パスフレーズ 入力確認

図4.2-7　セキュリティー（共通）WPA＋TKIP

表4.2-2　PSK 暗号キー入力一覧表

	入力可能文字数	入力可能文字
HEX	64 桁	16 進数
パスフレーズ	8～63 文字	半角英数字・半角記号（スペース、[?] は除く）

■WPA2 と TKIP、AES（CCMP）

認証方式として WPA2 を選択し、暗号化方式として TKIP と AES（CCMP） を Authentication サーバー使用で利用する場合は、以下を設定してください。

設定手順

手順1　〔SSID 編集〕画面（図 4.2-6）の〔セキュリティー（共通)〕をクリックします。

手順2　WPA2 と TKIP に関する設定を行います。

例として、下記内容での設定を示します。

- WPA2 〔有効〕を選択
- WPA/WPA2 認証方法〔802.1X〕を選択
- TKIP の〔有効〕を選択

TKIP 有効の場合、各無線インターフェース設定画面の〔運用動作モード設定〕で、TKIP の〔有効〕を選択してください。

※この設定変更では、設定反映後の保存とリセットが必要となります。

- AES 〔有効〕を選択

802.1X 認証を利用する場合、PSK の設定は無視されます。

「4.2.3 Authentication サーバーを利用した IEEE802.1X 認証」を参照ください。

CCMP を利用するには、上記設定画面で AES を有効にします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

セキュリティー(共通)

項目	設定
固定WEP	○有効 ◉無効
動的WEP	○有効 ◉無効
WEPキー *4	○WEP40 ◉WEP104 ◉ASCII ○HEX ●●●●●●●●●●●●●●●● □入力確認
WPA	○有効 ◉無効
WPA2	◉有効 ○無効
WPA/WPA2認証方法	◉802.1X ○PSK
TKIP *5	◉有効 ○無効
AES	◉有効 ○無効
PSK *6	○HEX ◉パスフレーズ ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●● □入力確認

図4.2-8　セキュリティー（共通）WPA2＋TKIP

認証方式と暗号化方式の可能な組み合わせを以下の表に示します。なお、固定 WEP、動的 WEP、WPA（TKIP）、WPA2（TKIP）、WPA（CCMP）、WPA2（CCMP）を組み合わせて設定することで、同一 SSID 上に複数の認証方式・暗号化方式の端末を混在させることも可能です。

表4.2-3　認証方式と暗号化方式の組み合わせ一覧

IEEE802.11 認証 / 認証方式	Open 認証	Shared 認証
なし	固定 WEP	固定 WEP
IEEE802.1X	動的 WEP	×
WPA	TKIP	×
	CCMP	×
	TKIP と CCMP	×
IEEE802.11i/WPA2	TKIP	×
	CCMP	×
	TKIP と CCMP	×

※ WPA および WPA 2 の認証方式は、PSK、IEEE802.1X のいずれでもかまいません。

4.2.3 Authenticationサーバーを利用したIEEE802.1X認証

IEEE802.1X 認証を使用するには、Authentication サーバーの設定が必要です。本装置では、独立した IP インターフェースを 16 個持つことができ、各 IP インターフェースに Authentication サーバーを 1 つずつ設定できます。（Authentication サーバー設定画面では、Web 認証と合わせて 32 個設定できます。）

以下に示す構成例では、SSID 名「SalesGroup」（SSID 値「SALES」）の認証方式に WPA2/IEEE802.1X が設定されています。ここでは、SSID 名「SalesGroup」を例に、IEEE802.1X 認証を利用し、Authentication サーバーによってユーザーを認証する方法を紹介します。

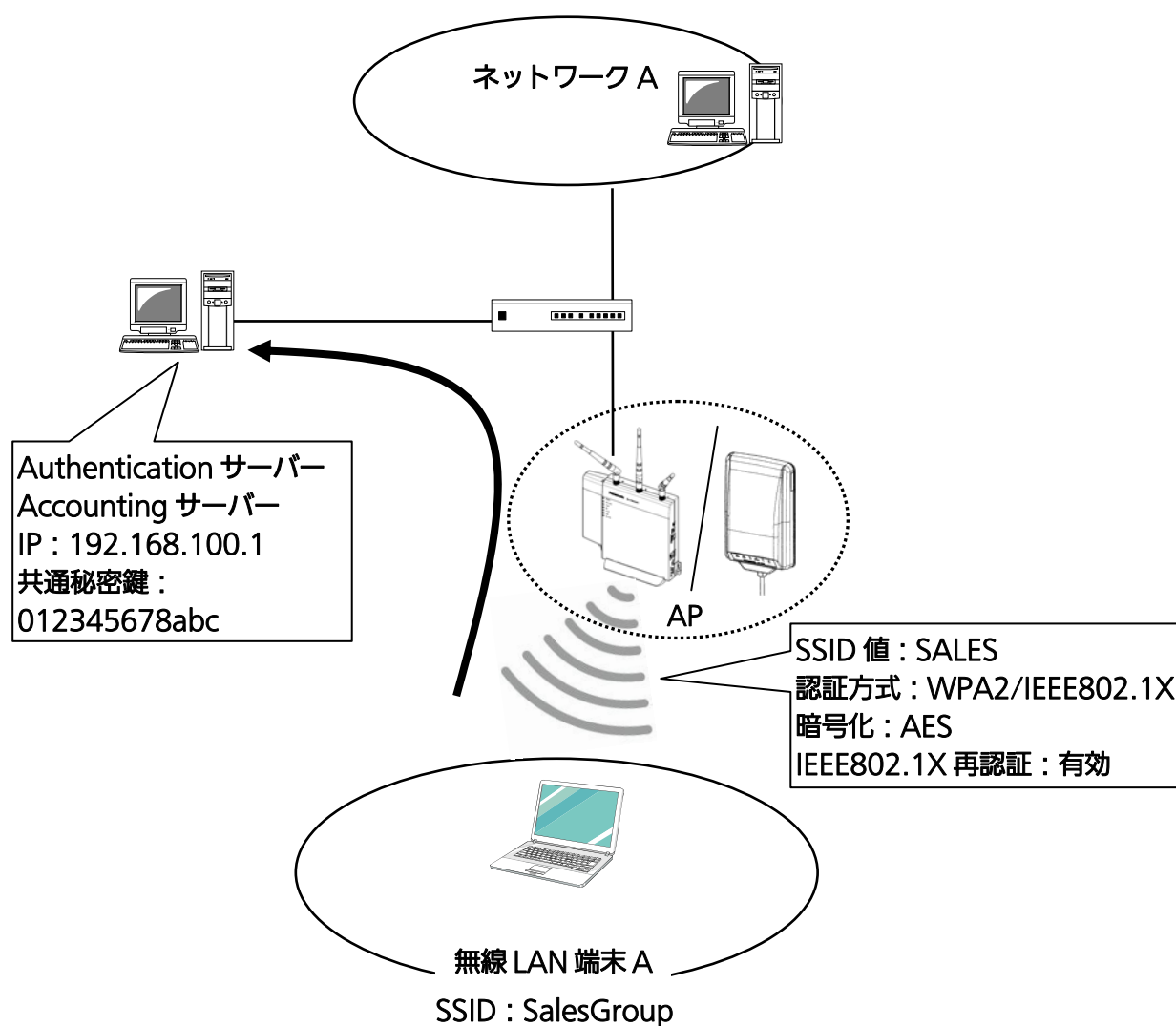



図4.2-9　認証サーバーを用いた環境構成例

設定手順

◆Authentication サーバーの設定

手順1　〔認証設定〕　→　〔認証サーバー設定〕　→　〔Authentication サーバー設定〕を
　　　クリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

認証サーバー設定　Authenticationサーバー設定

Web認証　Accountingサーバー設定

EA-7HW

図4.2-10　メニュー（Authentication サーバー設定）

手順2　〔Authentication サーバー一覧〕で設定するサーバーグループ番号の〔編集〕ボタンを
　　　クリックします。

例として、サーバーグループ番号：1 を選択します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

Authenticationサーバー設定

Authentication用RADIUSサーバーに関する設定を行います。

Authenticationサーバー一覧

サーバーグループ番号	現用サーバー	サーバー種別	接続	サーバー名	IP-IF No. *1	サーバーIPアドレス	送信先ポート番号	
1	Running	Running	無効		1	0.0.0.0	1812	編集
		Backup	無効		1	0.0.0.0	1812	
		Running	無効		1	0.0.0.0	1812	

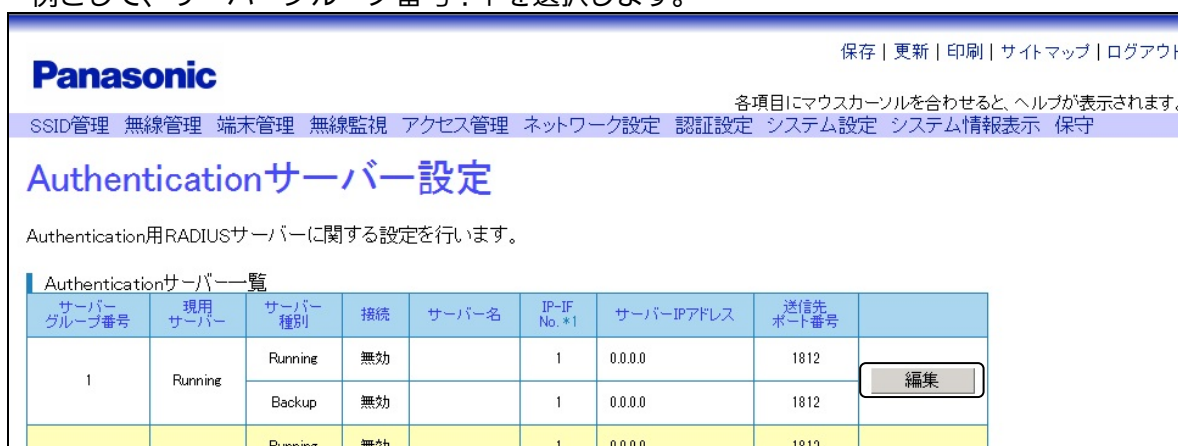



図4.2-11　Authentication サーバー設定

手順3　〔Running サーバー設定〕をクリックします。

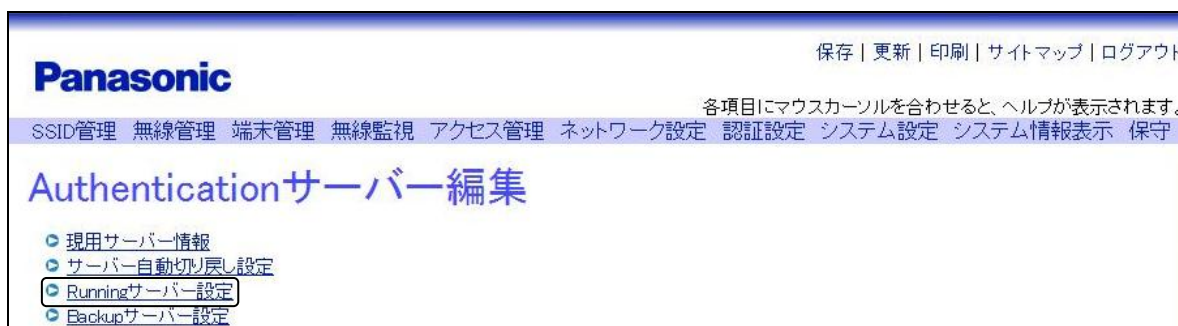



図4.2-12　Authentication サーバー編集

手順4　Authentication サーバーの設定を行います。

例として、下記内容での設定を示します。

- サーバー接続〔有効〕を選択
- サーバー名に「AUTH-01(MAIN)」を入力
- IP インターフェース番号〔1〕(Running サーバー接続に利用する自装置の IP インターフェース番号）を選択
- サーバーIP アドレスに「192.168.100.1」(Running サーバーの IP アドレス）を入力
- 送信先ポート番号の〔1812〕(対象となる Running サーバーの UDP ポート番号）を選択
- 共有秘密鍵に Running サーバーの共有秘密鍵「012345678abc」を入力（1 ～ 64 文字、半角英数字と半角記号（〔?〕は除く））
- サーバーによる端末制御〔有効〕を選択

図4.2-13　Running サーバー設定

手順5　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

※ Backup サーバーを利用する場合は、Backup サーバーに対しても同様の設定を行ってください。

◆Accounting サーバーの設定

Accounting サーバーも Authentication サーバーとあわせて設置されている場合

手順6　〔認証設定〕 → 〔認証サーバー設定〕 → 〔Accounting サーバー設定〕をクリックします。

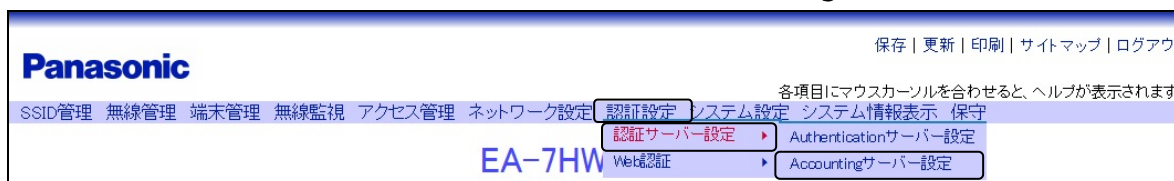



図4.2-14　メニュー（Accounting サーバー設定）

手順7　設定するサーバーグループ番号の〔編集〕ボタンをクリックします。

例として、サーバーグループ番号：1 を編集します。

図4.2-15　Accounting サーバー設定

手順8　〔Running サーバー設定〕をクリックします。

図4.2-16　Accounting サーバー編集

手順9　Accounting サーバーの設定を行います。

例として、下記内容での設定を示します。

- サーバー接続の〔有効〕を選択
- サーバー名に「ACCT-01(MAIN)」を入力
- IP インターフェース番号〔1〕（Running サーバー接続に利用する自装置の IP インターフェース番号）を選択
- サーバーIP アドレスに「192.168.100.1」（Running サーバーの IP アドレス）を入力
- 送信先ポート番号の〔1813〕（対象となる Running サーバーの UDP ポート番号）を選択
- 共有秘密鍵に Running サーバーの共有秘密鍵「012345678abc」を入力（1 ～ 64 文字、半角英数字と半角記号（〔?〕は除く））

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

Runningサーバー設定

サーバー接続	◉有効 ○無効
サーバー名 *1	ACCT-01(MAIN) (0～16文字)
IPインターフェース番号 一覧参照	1
サーバーIPアドレス	192.168.100.1 (xxx.xxx.xxx.xxx [xxx=0～255])
送信先ポート番号	◉1813 ○1646
共有秘密鍵 *2	●●●●●●●●●●●● (1～64文字) □ 入力確認

図4.2-17　Running サーバー設定

手順10　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させせます。

※ Backup サーバーを利用する場合は、Backup サーバーに対しても同様の設定を行ってください。

◆IEEE802.11i/WPA2 認証の設定

手順11 〔SSID 管理〕 → 〔SSID 設定〕を選択します。

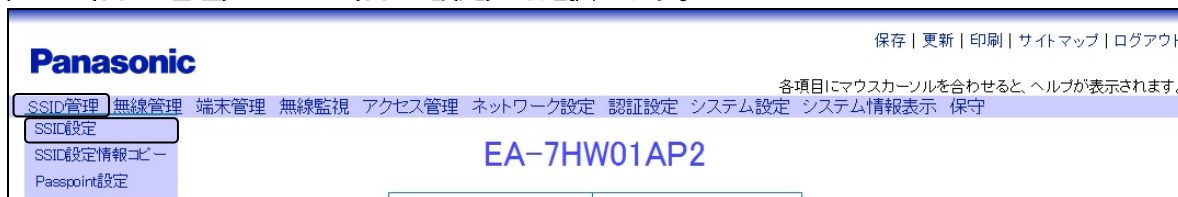



図4.2-18 メニュー（SSID 設定）

手順12 対象となる SSID の〔編集〕ボタンをクリックします。

図4.2-19 SSID 一覧

手順13 〔IEEE802.11 設定〕をクリックします。

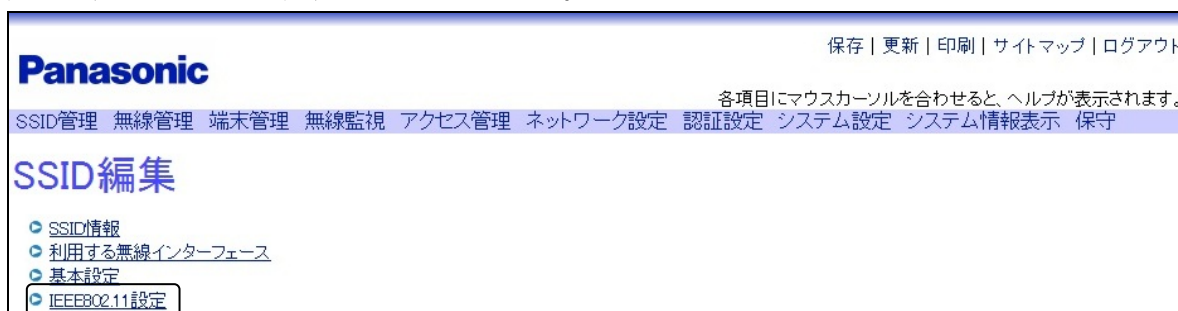



図4.2-20 SSID 編集（IEEE802.11 設定）

手順14 IEEE802.11 の設定を行います。
例として、802.11 認証アルゴリズム〔open〕を選択します。

図4.2-21 IEEE802.11 設定

手順15　〔SSID 編集〕画面の〔セキュリティー（共通）〕をクリックし、WPA2 の設定を行います。

下記内容での設定を示します。

- WPA2 〔有効〕を選択
- WPA/WPA2 認証方法〔802.1X〕を選択
- AES 〔有効〕を選択

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

セキュリティー(共通)

項目	設定
固定WEP	○有効 ◉無効
動的WEP	○有効 ◉無効
WEPキー *4	◉WEP40 ○WEP104 ◉ASCII ○HEX ●●●●●●●●●●●● □入力確認
WPA	○有効 ◉無効
WPA2	◉有効 ○無効
WPA/WPA2認証方法	◉802.1X ○PSK
TKIP *5	◉有効 ○無効
AES	◉有効 ○無効
PSK *6	◉HEX ○パスフレーズ ●● □入力確認

図4.2-22　セキュリティー（共通）

手順16　〔SSID 編集〕画面の〔IEEE802.1X 設定〕をクリックし、再認証実行を〔有効〕にします。

図4.2-23　IEEE802.1X 設定

手順17　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

◆SSID で使用する Authentication サーバーの設定

手順18 〔SSID 編集〕画面の〔Authentication・Accounting（MAC 認証/EAP 認証）〕をクリックし、Authentication サーバーの設定を行います。

例として、下記内容での設定を示します。

- ・ 使用 Authentication サーバー番号に“1”（手順 2 で指定したサーバー番号）を選択
- ・ NAS-ID に「nasidxxxx」を入力

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

Authentication・Accounting(MAC認証/EAP認証)

使用Authenticationサーバー番号 一覧参照	1
使用Accountingサーバー番号 一覧参照	1
Accounting機能使用	◉使用する ○使用しない
NAS-ID *9	nasidxxxx (0～253文字)
Interim動作種別	○定周期動作 ◉サーバーからの要求時のみ ○OFF
Interim送信間隔	86400 秒 (60～86400(3600×24))
MACアドレス区切り文字	◉省略 ○コロン ○ハイフン ○ドット (2byte単位)

図4.2-24 Authentication ・Accounting（MAC 認証/EAP 認証）

手順19 画面最下部の〔設定〕ボタンをクリックします。

以上で、Authentication サーバーを使った WPA2 認証設定は完了です。

4.2.4 ユーザー認証

■ユーザー認証 VLAN

ユーザー認証 VLAN では、IEEE802.1X 認証により、無線 LAN 端末のユーザーを基準にして、トラフィックを VLAN 分離することが可能となります。ここでは、以下の図に示すユーザー認証 VLAN ネットワークの設定方法を紹介します。

たとえば、ネットワーク A のユーザーには、Authentication サーバーによる認証の結果 VLAN-ID=100 が発行されて、ネットワーク A への接続が可能となります。また、ネットワーク B ユーザーには、VLAN-ID=200 が発行され、ネットワーク B への接続が可能となります。

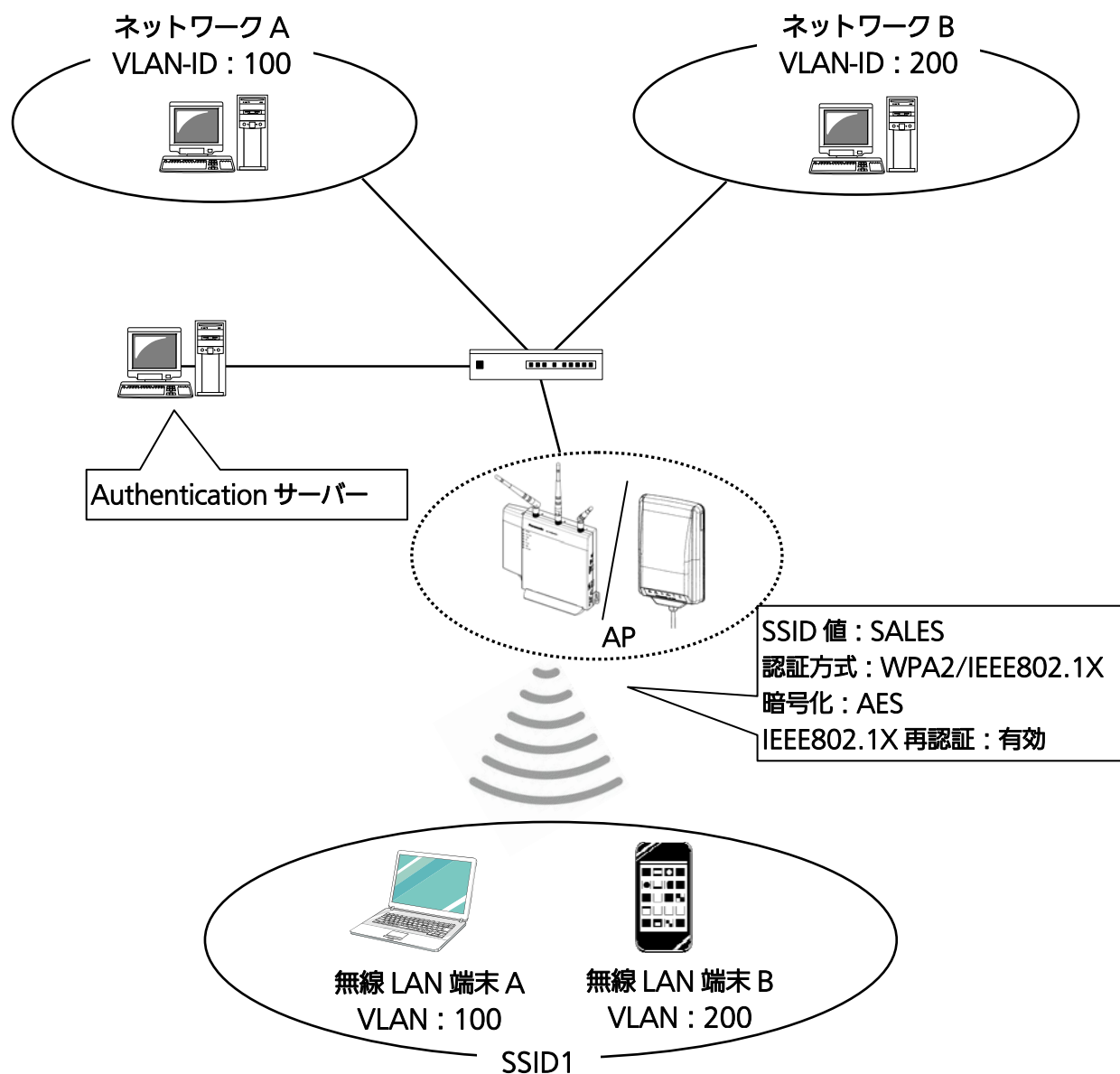
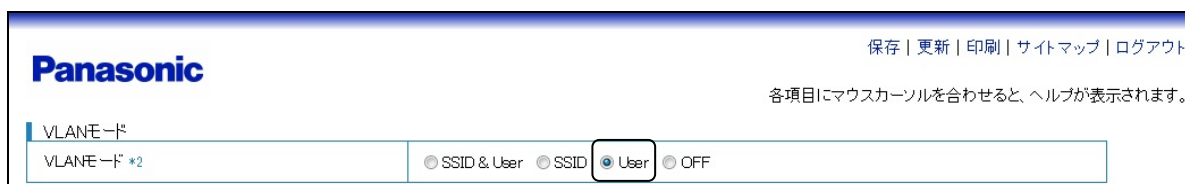



図4.2-25　環境例（ユーザー認証 VLAN）

Authentication サーバーの設定方法については、「4.2.3　Authentication サーバーを利用した IEEE802.1 認証」内の「■Authentication サーバー」を参照してください。

また、各ユーザーに対して発行される VLAN-ID は、Authentication サーバー側にあらかじめ設定を行っておいてください。設定方法は、Authentication サーバーの取扱説明書を参照してください。

ユーザー認証 VLAN では、それぞれの VLAN 設定を行い、VLAN モードで〔User〕を選択します。

図4.2-26　 VLAN モード選択

以上で、ユーザー認証 VLAN の設定は完了です。

■ユーザー認証 VLAN ＋ SSID VLAN

SSID ごとに VLAN を分離したうえで、さらにユーザー認証 VLAN により無線 LAN 端末ごとに VLAN を分離することが可能となります。

ネットワーク A とネットワーク B とで VLAN 分離を行ったうえで、さらに管理用と一般用をユーザー認証 VLAN で分けるような設定が可能です。このような二重の VLAN 構成を実現するためには、SSID に対して拡張 VLAN（ダブルタグ VLAN）の設定を行ってください。

下記の構成例では、端末からのトラフィックは、はじめに SSID にマッピングされた VLAN-ID（100 or 200）によって部門ごとに分離された後、Authentication サーバーによって割り当てられるユーザー認証 VLAN-ID（10 or 20）によって管理用ネットワークまたは一般用ネットワークのいずれかに分離されます。

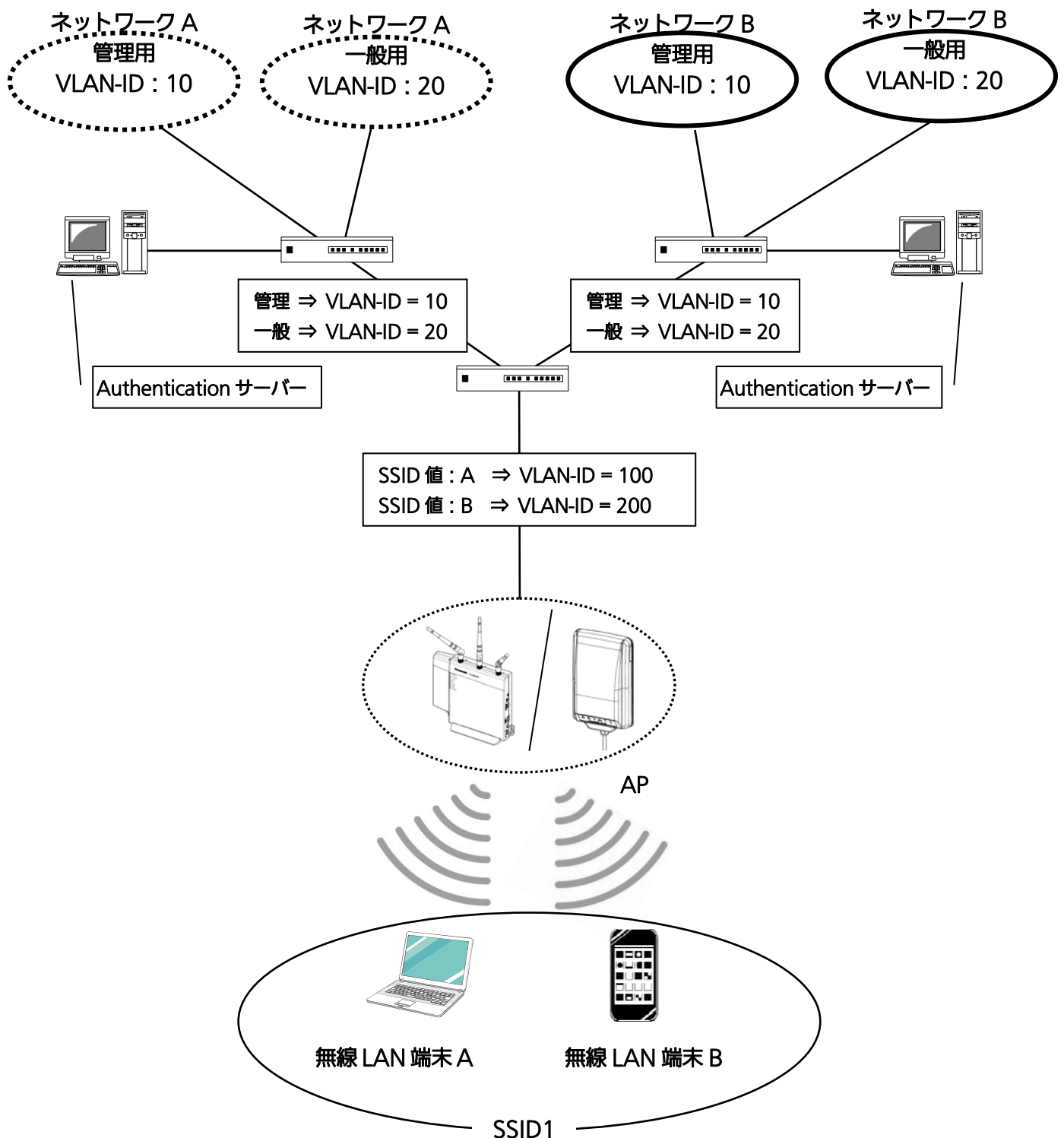



図4.2-27 構成例（ユーザー認証 VLAN ＋ SSID VLAN）

Authentication サーバーの設定方法については、「4.2.3　Authentication サーバーを利用したIEEE802.1X 認証」内の「■Authentication サーバー」を参照してください。
また、各ユーザーに対して発行される VLAN-ID は、Authentication サーバー側にあらかじめ設定を行っておいてください。

ユーザー認証 VLAN ＋ SSID VLAN では、それぞれの VLAN 設定を行い、VLAN モードで〔SSID ＆ User〕を選択します。

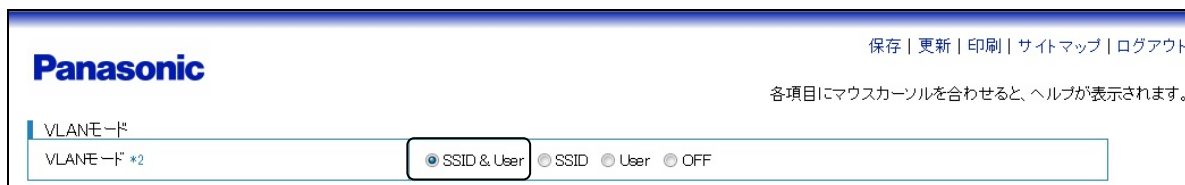



図4.2-28 VLAN モード（SSID 設定）

以上で、ユーザー認証 VLAN ＋ SSID VLAN の設定は完了です。

4.3　自動干渉回避

本装置では、無線伝送路の干渉状態を観測し、得られた結果をもとに送受信チャネルを自動的に選択・変更して干渉を回避することができます。

送受信チャネルの自動選択の場合、干渉が観測されても、すぐに干渉の自動回避が行われるわけではなく、特定の電界強度以上の状態が 6 分間以上続くと干渉ありと判断されます。その後 特定の電界強度以下の状態が 6 分間以上続くと、干渉なしと判断されます。（特定の電界強度：干渉波＝－60 dBm、干渉 AP＝－70 dBm ）

4.3.1　送受信チャネル自動変更

802.11b/g/n 設定を例に、送受信チャネルの自動変更の設定方法を紹介します。

設定手順

◆送受信チャネルの自動変更の設定

ここでは 2.4GHz 帯設定を例に説明します。

手順1　〔無線管理〕　→　〔2.4GHz 帯設定〕を選択します。

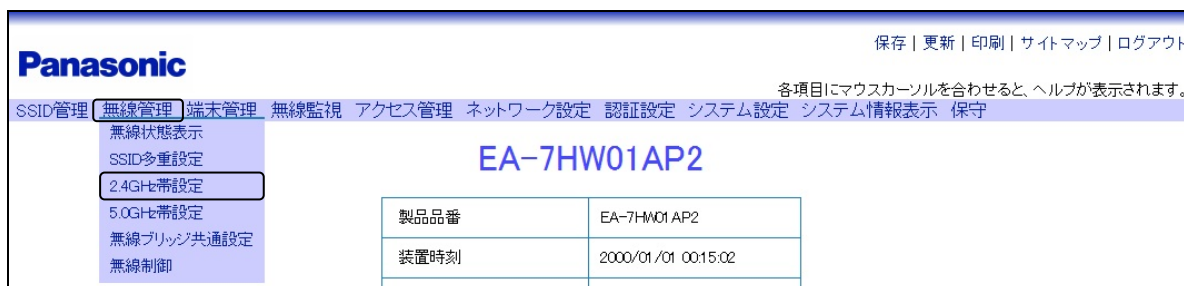



図4.3-1 メニュー（2.4GHz 帯設定）

手順 2 ～ 手順 4 は〔2.4GHz 帯設定〕画面（図 4.3-2）より各種設定を行います。

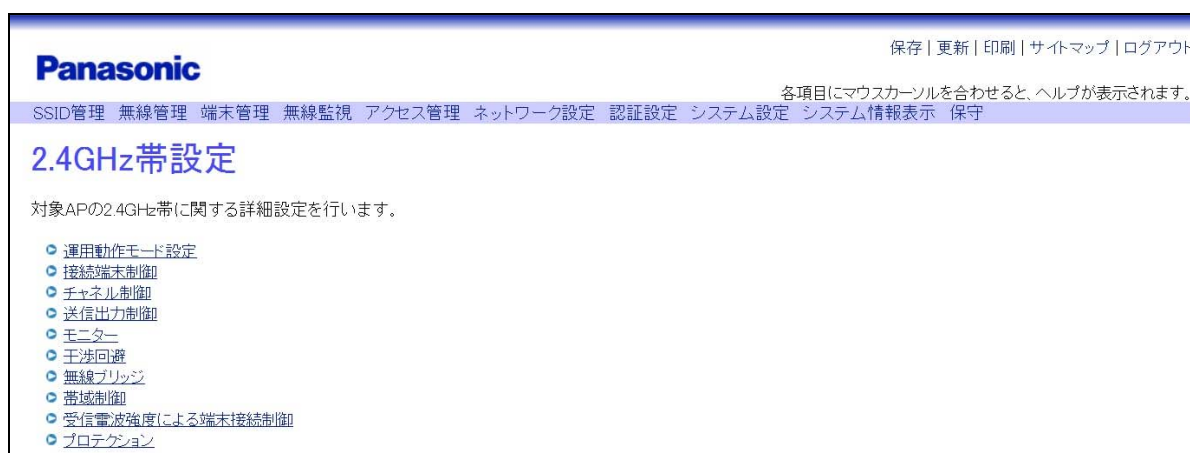



図4.3-2　2.4GHz 帯設定

手順2　〔2.4GHz 帯設定〕画面（図 4.3-2）の〔運用動作モード設定〕をクリックし、
無線インターフェースの動作と動作モードを設定します。

例として、下記内容での設定を示します。

- 無線インターフェース〔有効〕を選択
- 動作モード〔通常運用〕を選択
  ※動作モードの設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

〔無線モニター〕を選択した場合、その無線 LAN アクセスポイントへの端末接続はできなくなり、監視のみが行われます。

図4.3-3 運用動作モード設定

手順3　〔2.4GHz 帯設定〕画面（図 4.3-2）の〔チャネル制御〕をクリックし、チャネル制御モードと優先チャネル番号を設定します。

例として、下記内容での設定を示します。

- チャネル制御モード：〔自動〕を選択
- チャネル番号：〔1〕を選択
- 選択可能チャネル（1ch ～ 13ch）：〔選択可能にする〕を選択

図4.3-4　チャネル制御

重要	■ W52（36ch～48ch）、W53（52ch～64ch）は、電波法により屋内使用限定です。屋外使用の場合、チャネル番号設定には、「36ch～64ch」を選択しないでください。また、チャネル制御モードが自動設定の場合、選択可能チャネル設定については、「36ch～64ch」は、「選択可能にしない」を選択してください。

手順4　〔2.4GHz 帯設定〕画面（図 4.3-2）の〔干渉回避〕をクリックし、干渉検出時最終動作を選択します。

例として、干渉検出時最終動作の〔スタンバイ〕を選択します。

図4.3-5　干渉回避

手順5　画面最下部の〔設定〕ボタンをクリックします。

※他システムからの干渉検出時の最終動作には、以下の 2 種類があります。
・スタンバイ：利用可能周波数がないためモニター動作を行う。
・運用：一番影響の少ない周波数を選択して動作を続ける。
また、無線中継モード（無線ブリッジ）を使用すると、クライアント AP はその無線インターフェースでの自動干渉回避はできません（サーバーAP は自動干渉回避します）。

4.3.2　隣接AP・干渉APの確認

本装置は、使用チャネルの「常時監視」(スタンバイ、もしくは監視モードである場合は、全チャネルの「常時監視」)を行います。監視の結果は各種状態として表示するとともに、これを元に干渉検出・干渉回避、レーダー検出・回避などの処理を行います。
2.4GHz の無線インターフェースでは 1ch〜14ch、5GHz の無線インターフェースでは 36ch〜140ch を監視します。

操作手順

◆隣接 AP

手順1　〔無線監視〕　→　〔隣接 AP〕を選択します。

図4.3-6　メニュー(隣接 AP)

手順 2 〜 手順 6 は〔隣接 AP〕画面(図 4.3-7)より各種操作を行います。

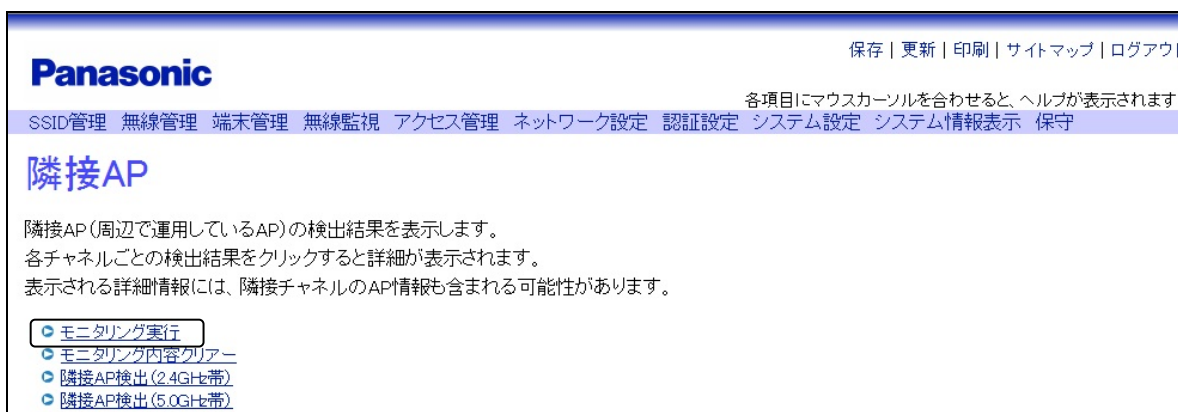



図4.3-7　隣接 AP

手順2　〔隣接 AP〕画面にて、モニタリング実行をクリックし、〔実行〕ボタンをクリックします。

図4.3-8　モニタリング実行

手順3　〔モニタリング実行確認〕のダイアログボックスで〔OK〕をクリックします。

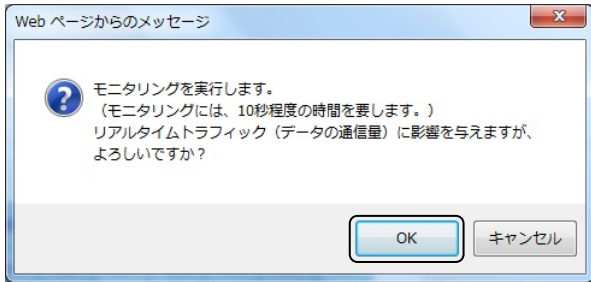



図4.3-9　モニタリング実行確認

手順4　〔モニタリング実行受付〕のダイアログボックスで〔OK〕をクリックします。

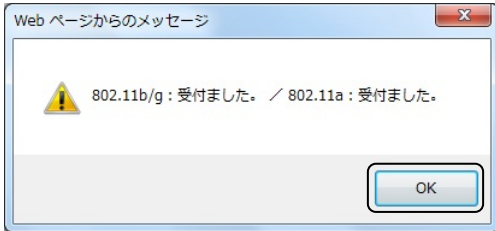



図4.3-10　モニタリング実行受付

手順5　〔隣接 AP 検出（2.4GHz 帯）〕または〔隣接 AP 検出（5.0GHz 帯）〕をクリックします。
手順6　隣接 AP 検出結果欄の“○”または“ - ”をクリックします。（図 4.3-11）

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

隣接AP検出(2.4GHz帯)

チャネルごとの隣接AP *1													
1ch	2ch	3ch	4ch	5ch	6ch	7ch	8ch	9ch	10ch	11ch	12ch	13ch	14ch
○	○	－	－	－	○	－	－						

*1　隣接APを検出した場合は「○」、検出しなかった場合は「－」、
検出中またはモニタリング未実施である場合は「 」(空白)が表示されます。
モニタリング結果の詳細を表示する場合は、「○」をクリックしてください。
「 」(空白)の場合は、更新をクリックすることで検出中のモニタリング結果が表示されます。

このページのTopへ

隣接AP検出(5.0GHz帯)

チャネルごとの隣接AP *2																		
36ch	40ch	44ch	48ch	52ch	56ch	60ch	64ch	100ch	104ch	108ch	112ch	116ch	120ch	124ch	128ch	132ch	136ch	140ch
○	－	○	－	－	－	○	－											

*2　隣接APを検出した場合は「○」、検出しなかった場合は「－」、
検出中またはモニタリング未実施である場合は「 」(空白)が表示されます。
モニタリング結果の詳細を表示する場合は、「○」をクリックしてください。
「 」(空白)の場合は、更新をクリックすることで検出中のモニタリング結果が表示されます。

このページのTopへ

図4.3-11　隣接 AP 検出

手順 6 で隣接 AP 検出結果欄の “○” または “ - ” をクリックすると、下記画面（図 4.3-12）が表示されます。

モニタリング結果

検出AP情報

チャネル番号	1 ch

並べ替え

並べ替え	最新時刻

実行

モニタリング結果一覧

最新時刻	BSSID	SSID値（先頭の16文字を表示します）	RSSI値	プライマリチャネル	セカンダリチャネル	接続種別（11n/レガシー）
2000/01/01 00:05:36	00-22-EB-00-08-0F	PSSIS_WLANTEST_5	82	3	*	レガシー
2000/01/01 00:05:36	00-22-EB-00-08-00	PSSIS_WLANTEST_5	82	3	*	レガシー
2000/01/01 00:05:36	00-22-EB-00-08-07	PSSIS_WLANTEST_5	82	3	*	レガシー
2000/01/01 00:05:36	00-22-EB-00-73-07	PSSIS_WLANTEST_5	80	3	*	11n

図4.3-12　　隣接 AP モニタリング結果

◆干渉 AP

手順1　〔無線監視〕　→　〔干渉 AP〕を選択します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

隣接AP
干渉AP

EA-7HW01AP2

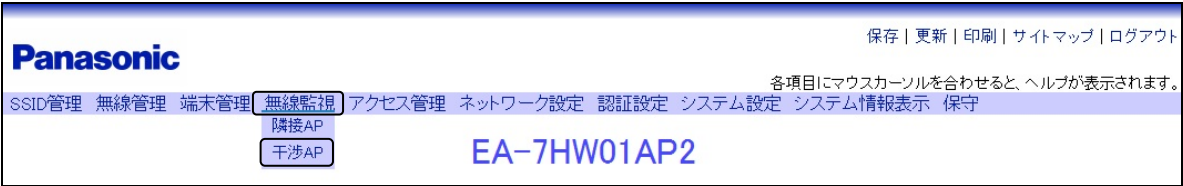



図4.3-13　メニュー（干渉 AP）

手順2　〔干渉 AP 検出（2.4GHz 帯）〕または〔干渉 AP 検出（5.0GHz 帯）〕をクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

干渉AP

干渉しているAPの検出結果を表示します。
各チャネルごとの検出結果をクリックすると詳細が表示されます。
表示される詳細情報には、隣接チャネルのAP情報も含まれる可能性があります。

- モニタリング内容クリアー
- 干渉AP検出(2.4GHz帯)
- 干渉AP検出(5.0GHz帯)

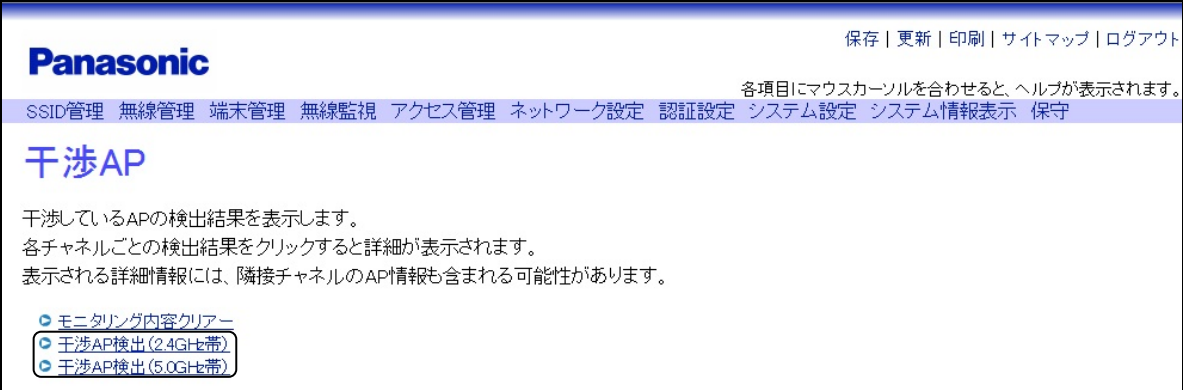



図4.3-14　干渉 AP

手順3　干渉 AP 検出結果欄の“○”または“ - ”をクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

干渉AP検出(2.4GHz帯)

チャネルごとの干渉AP *1													
1ch	2ch	3ch	4ch	5ch	6ch	7ch	8ch	9ch	10ch	11ch	12ch	13ch	14ch
○	−	○	−	−	○	−	−	○	−	○	−	−	−

*1　干渉APを検出した場合は「○」、検出しなかった場合は「−」が表示されます。
モニタリング結果の詳細を表示する場合は、「○」をクリックしてください。

このページのTopへ

干渉AP検出(5.0GHz帯)

チャネルごとの干渉AP *2																		
36ch	40ch	44ch	48ch	52ch	56ch	60ch	64ch	100ch	104ch	108ch	112ch	116ch	120ch	124ch	128ch	132ch	136ch	140ch
○	−	○	−	−	−	−	○	−	−	−	−	−	−	−	−	−	−	−

*2　干渉APを検出した場合は「○」、検出しなかった場合は「−」が表示されます。
モニタリング結果の詳細を表示する場合は、「○」をクリックしてください。

図4.3-15　干渉 AP 検出

手順 3 で干渉 AP 検出結果欄をクリックすると、下記画面（図 4.3-16）が表示されます。

最新時刻	BSSID	SSID値（先頭の16文字を表示します）	RSSI値	プライマリチャネル	セカンダリチャネル	接続種別（11n/レガシー）
2005/12/10 07:50:30	WWWWWWWW-35-C2-01	WWWWWWWWWWWWWWWW	30	1	2	11n
2005/12/10 10:06:08	00-00-EB-35-C2-02	HotSpot	50	1	2	レガシー
2005/12/10 07:50:30	00-00-EB-35-C2-03	Panasonic	0	1	14	レガシー
2005/12/10 09:27:50	00-00-EB-35-C2-04	HotSpot	70	1	64	レガシー

図4.3-16　干渉 AP モニタリング結果

4.3.3 レーダー監視

レーダー監視の概要

本装置は、各種レーダーと共用する 5GHz 帯 MiddleBand 5.25～5.35GHz（W53）、および 5.47～5.725GHz（W56）のチャネルに対応しているため、各種レーダーを監視する機能を備えています。5GHz 帯の無線インターフェースで 52,56,60,64,100,104,108,112,116,120,124,128,132,136,140 チャネル（以下、レーダー監視対象チャネル）を設定した場合、レーダー監視機能（起動時・運用中の動作）を自動的に動作させます。

起動時の動作

装置の起動時にレーダー監視対象チャネルのいずれかが選択されていた場合、各種レーダー波検出を 1 分間行います。各種レーダーを検出した場合は、TRAP にて通知を行い（設定がされていた場合のみ）、適切な送受信チャネルを選択し自動変更します。選択されたチャネルもレーダー監視対象チャネルのいずれかである場合は、同様に 1 分間のレーダー確認を行い、以後これを繰り返し、最終的にレーダーが検出されないチャネルを選択します。
送受信チャネルが固定で設定されていた場合、最終動作設定が「強制送信」設定でも、レーダー波検出後 30 分間のスタンバイ状態になります。30 分後に改めて起動時の動作を行います。
また、装置の起動時に本機能が動作するため、装置が動作するまでに約 2 分程度時間がかかります。

運用中の動作

各種レーダーが検出されずレーダー監視対象チャネルのいずれかのチャネルで運用を開始したとしても、その使用チャネルでの各種レーダー波検出を行います。各種レーダー波を検出した場合、TRAP にて通知を行い（設定がされていた場合のみ）、その無線 LAN アクセスポイント配下のすべての端末に Deauthentication を送信し端末の切断を行って、起動時と同様の動作をします。
5GHz 帯の無線インターフェースでレーダー監視対象チャネルを設定した場合、本機能は自動的に有効になります。設定を変更することはできません。

4.3.4 周波数帯域幅復旧

周波数帯域幅が 20 MHz /40MHz に設定されている場合に、チャネル選択時もしくは、セカンダリチャネル側のレーダー検出もしくは、セカンダリチャネル側の干渉波検出により、周波数帯域幅が 20MHz に決定した場合は、「40MHz 復旧幅監視間隔」毎に、チャネル選択を実施し、20 MHz /40MHz で運用可能な周波数を検索します。
ただし、「周波数自動制御」設定が固定で、運用周波数が 140ch の場合は、20/40MHz 運用できないため、「40MHz 復旧幅監視間隔」にかかわらず、復旧処理は行いません。
5GHz 帯でのみ 40MHz 運用が可能なため本設定も 5.0GHz メニューでのみ有効化されています。

設定手順

◆周波数帯域幅復旧設定

手順1 〔無線管理〕 → 〔5.0GHz 帯設定〕を選択します。

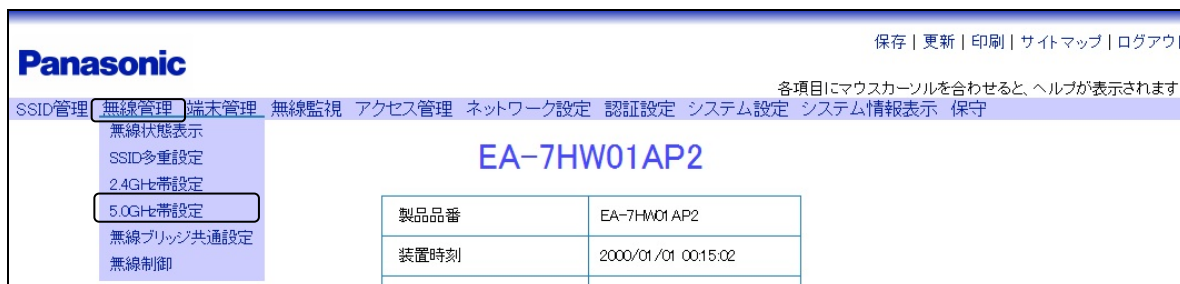



図4.3-17 メニュー（5.0GHz 帯設定）

手順2 〔チャネル制御〕をクリックします。

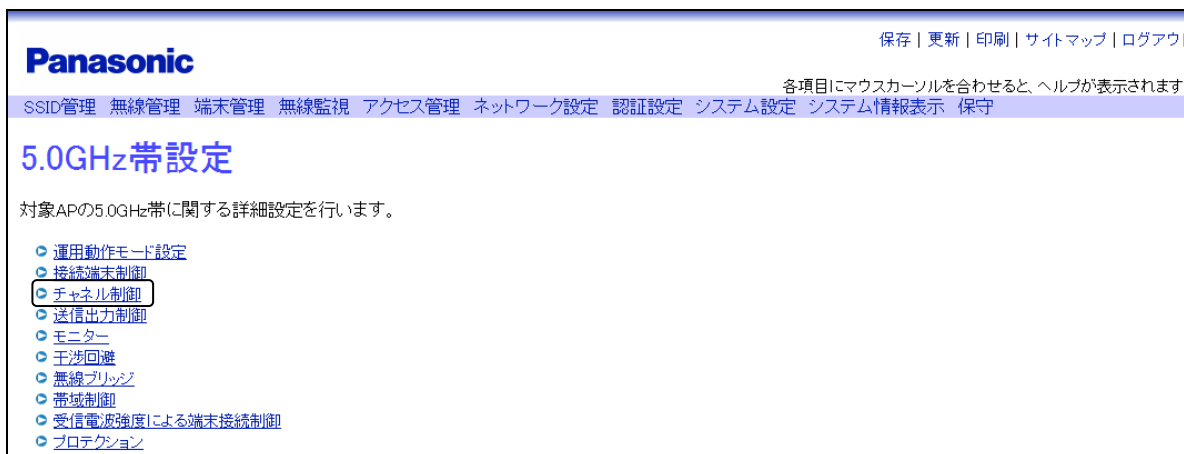



図4.3-18 5.0GHz 帯設定

手順3　〔チャネル制御モード〕、〔周波数帯域幅〕、〔40MHz 復旧監視機能〕、〔40MHz 復旧監視間隔〕を設定します。

例として、下記内容での設定を示します。

- チャネル制御モード　　　:〔自動〕を選択
- 周波数帯域幅　　　　　　: [20MHz/40MHz]を選択
- 40MHz 復旧監視機能　　 : [有効]を選択
- 40MHz 復旧監視間隔　　 : [30]分を入力

※ 40MHz 復旧監視機能を[有効]にした場合、モニター機能（3.6　各無線インターフェースの設定参照）と同様の動作を行うため、パケットロスが発生したり、接続した端末が切断される可能性があります。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

チャネル制御

チャネル制御モード		○固定 ◉自動
チャネル番号 *3 *4		36
選択可能チャネル *5	36ch	◉選択可能にする ○選択可能にしない
	40ch	◉選択可能にする ○選択可能にしない
	44ch	◉選択可能にする ○選択可能にしない
	48ch	◉選択可能にする ○選択可能にしない
	52ch	◉選択可能にする ○選択可能にしない
	56ch	◉選択可能にする ○選択可能にしない
	60ch	◉選択可能にする ○選択可能にしない
	64ch	◉選択可能にする ○選択可能にしない
	100ch	◉選択可能にする ○選択可能にしない
	104ch	◉選択可能にする ○選択可能にしない
	108ch	◉選択可能にする ○選択可能にしない
	112ch	◉選択可能にする ○選択可能にしない
	116ch	◉選択可能にする ○選択可能にしない
	120ch	◉選択可能にする ○選択可能にしない
	124ch	◉選択可能にする ○選択可能にしない
	128ch	◉選択可能にする ○選択可能にしない
	132ch	◉選択可能にする ○選択可能にしない
	136ch	◉選択可能にする ○選択可能にしない
	140ch	◉選択可能にする ○選択可能にしない
周波数帯域幅		○20MHz ◉20MHz/40MHz
40MHz復旧監視機能 *6		◉有効 ○無効
40MHz復旧監視間隔		30 分 (1～1440)

図4.3-19　チャネル制御（5GHz）

手順4　画面最下部の〔設定〕ボタンを押し、設定を反映させせます。

4.4 フィルタリング

本装置では、ユーザーからのデータフレーム（無線 LAN 端末への無線 LAN 送信フレーム及び、無線 LAN 端末からの無線 LAN 受信フレーム、無線 LAN アクセスポイントからの無線ブリッジフレーム）に対して、MAC レイヤーでのフィルタリング、IP レイヤーでのフィルタリングを行うことができます。
また、ユーザーデータのフィルタリングとは別に、管理用 IP インターフェースごとに、管理フレーム（Admin フレーム：装置宛てのフレーム）をフィルタリングすることもできます。

■ブリッジフィルター条件
以下の条件を基に、MAC レイヤーのフィルタリング条件（アクセスリスト）が設定できます。アクセスリストは 512 個設定することができます。
① イーサタイプ
② 送信元 MAC アドレス
③ 送信先 MAC アドレス
④ CoS 値（802.1p プライオリティ）（=/</>の指定可能）
上記条件の破棄・透過の設定を複数エントリーすることが可能です。
①～④の各条件に対してすべてを受け入れる指定も可能です。

■IP フィルター条件
以下の条件を基に、IP レイヤーのフィルタリング条件（アクセスリスト）適用の有無が設定できます。
アクセスリストは 512 個設定することができます。

① IP プロトコル種別
② 送信元ネットワークアドレス
フルアドレスマスクにより　ホストの指定も可能（マスクは中抜き可能）
③ 宛先ネットワークアドレス
フルアドレスマスクにより　ホストの指定も可能（マスクは中抜き可能）
④ 送信元 UDP／TCP ポート番号（=/</>の指定可能）
⑤ 送信先 UDP／TCP ポート番号（=/</>の指定可能）
⑥ TOS 値（=/</>の指定可能）
上記条件の破棄・透過の設定を複数エントリーすることが可能です。
①～⑥の各条件に対してすべてを受け入れる指定も可能です。

■PPPoE フィルター条件
PPPoE フレームへの IP レイヤーフィルタリング条件（アクセスリスト）が設定できます。SSID 単位、もしくは無線ブリッジ時における VLAN-ID 単位で設定が可能です。

ここでは、無線 LAN 端末宛ての Ethernet フレームに対するフィルター設定を説明します。

設定手順

◆フィルター設定（ブリッジフィルター条件）

手順1　〔アクセス管理〕　→　〔アクセス制御リスト編集〕　→　〔ブリッジ条件設定〕を選択します。

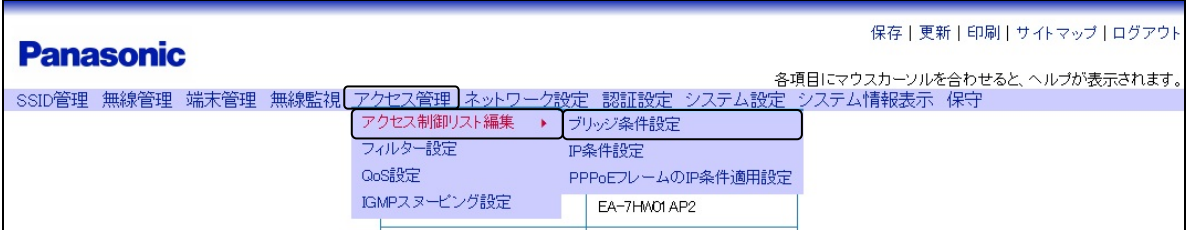



図4.4-1 メニュー（ブリッジ条件設定）

手順2　〔編集〕ボタンをクリックします。

ブリッジ条件設定

MACレイヤーのアクセスリスト条件を編集します。
この条件は、フィルター設定、優先設定、CoS値設定およびTOS値設定で使用します。
条件は最大で512個登録することができます。

条件一覧

No.	状態	種別	送信元MACアドレス	送信先MACアドレス	イーサタイプ	CoS値		
1	有効	破棄	11-00-00-11-12-2C	00-00-56-C1-11-DA	CCCC	=7	編集	削除
2	有効	透過	00-00-EB-11-22-30	00-0D-56-C1-11-DA	CCCC	=7	編集	削除
3	無効	透過	*	*	*	*	編集	削除

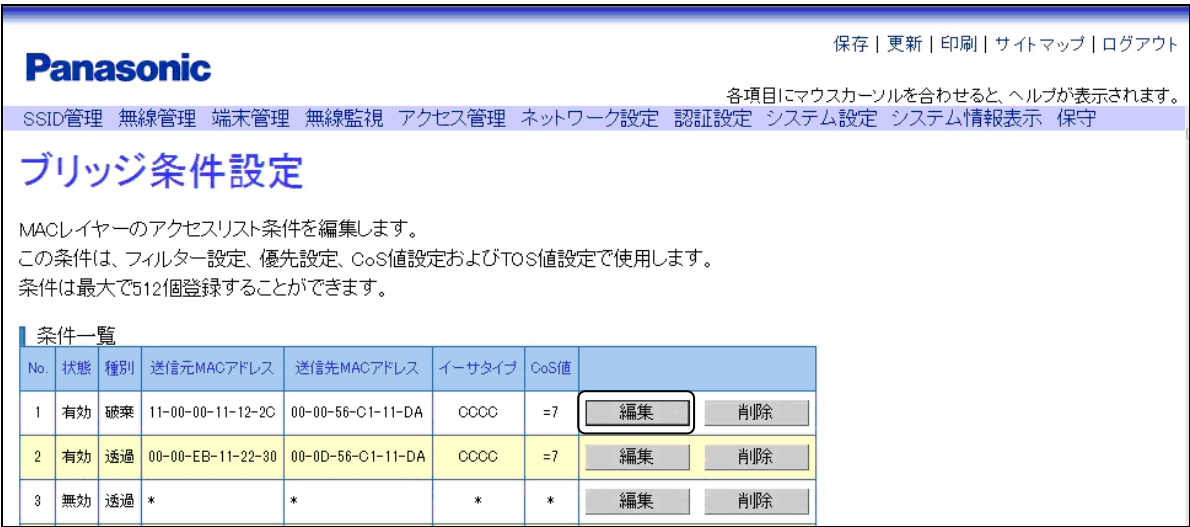



図4.4-2　ブリッジ条件設定

手順3　ブリッジ条件を登録します。

例として、下記内容での設定を示します。

- 実施種別に〔破棄〕を選択（下記条件に合ったものを破棄します。）
- 送信元 MAC アドレスは、「11-00-00-11-12-2C」を入力
- 送信先 MAC アドレスは、「00-0D-56-C1-11-DA」を入力
- イーサタイプは「CCCC」を入力
- CoS 値は「=7」を入力

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

ブリッジ条件編集

ブリッジ条件番号

条件番号	1

条件内容

実施種別 *4 *5 *6	◎透過 ◉破棄
送信元MACアドレス *1 *7	11-00-00-11-12-2C
送信先MACアドレス *1 *7	00-0D-56-C1-11-DA
イーサタイプ *1	CCCC （HEX:0000～FFFF）
CoS値 *1 *2 *3 *5	=7 （0～7）

図4.4-3　ブリッジ条件編集

手順4　画面最下部の〔設定〕ボタンをクリックします。

手順5　〔アクセス管理〕 → 〔フィルター設定〕　を選択します。

図4.4-4　メニュー（フィルター設定）

手順6　〔フィルター制御（無線 LAN 送信)〕をクリックし、〔フィルター制御（無線 LAN 送信)〕選択で〔ブリッジ条件〕をクリックします。

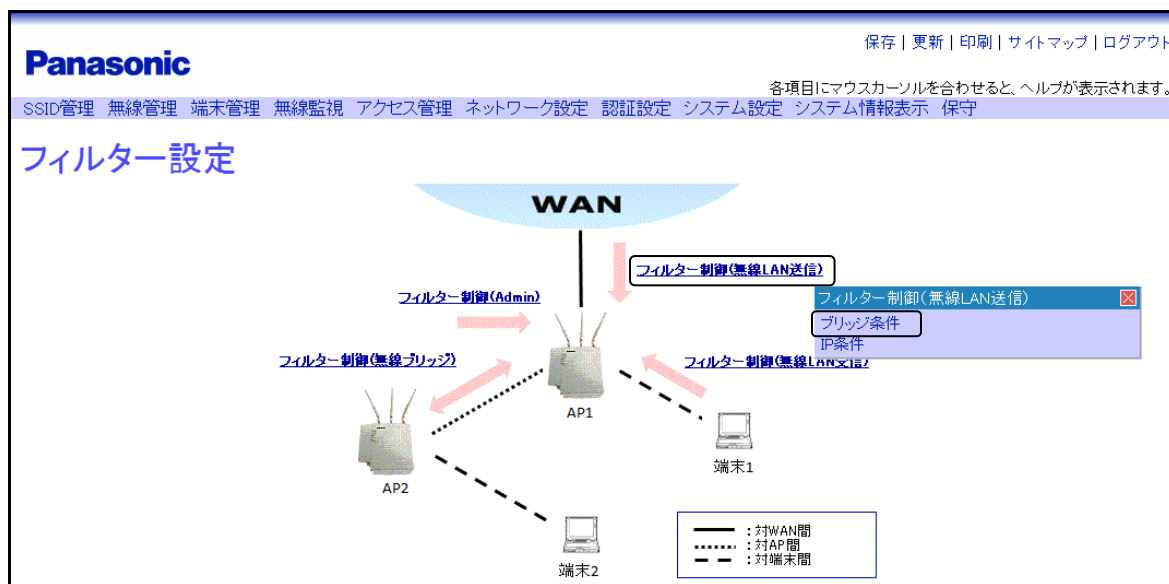



図4.4-5　フィルター設定(屋内用無線 LAN アクセスポイント)

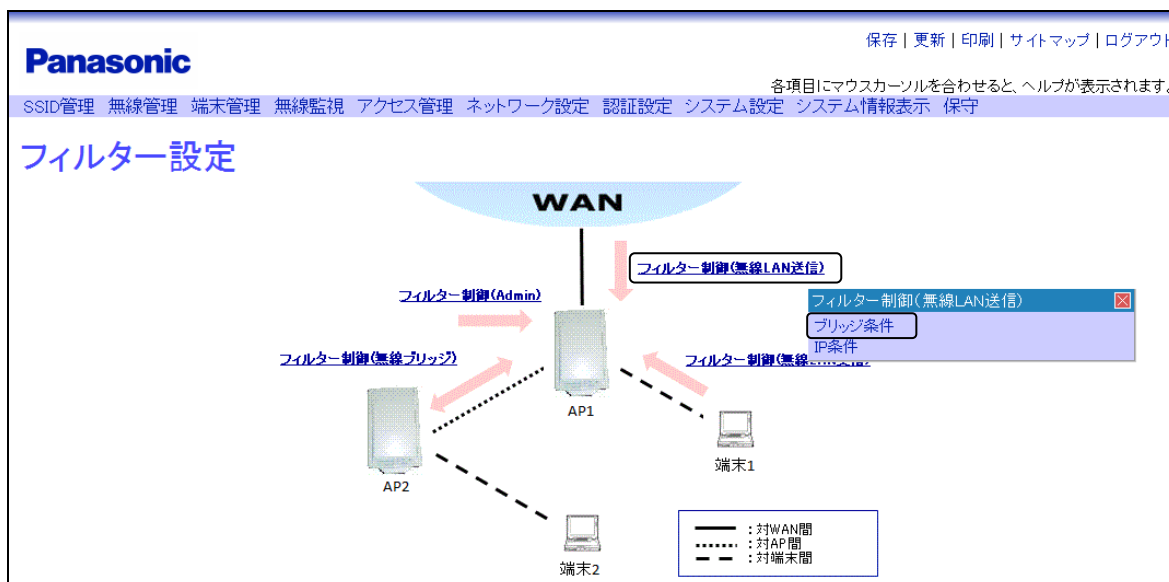



図4.4-6　フィルター設定(屋外用無線 LAN アクセスポイント)

手順7　ブリッジフィルター設定するSSID番号をドロップダウンリストから選択し、〔表示〕ボタンをクリックします。

図4.4-7　SSID選択

手順７で〔表示〕ボタンをクリックすると、下記画面が表示されます。(図 4.4-8)

図4.4-8　登録済みフィルター条件一覧

手順8　ブリッジフィルター条件番号を入力し、〔登録〕ボタンをクリックします。

図4.4-9　ブリッジフィルター条件登録

◆フィルター設定（IP フィルター条件）

手順1　〔アクセス管理〕　→　〔アクセス制御リスト編集〕　→　〔IP 条件設定〕を選択します。

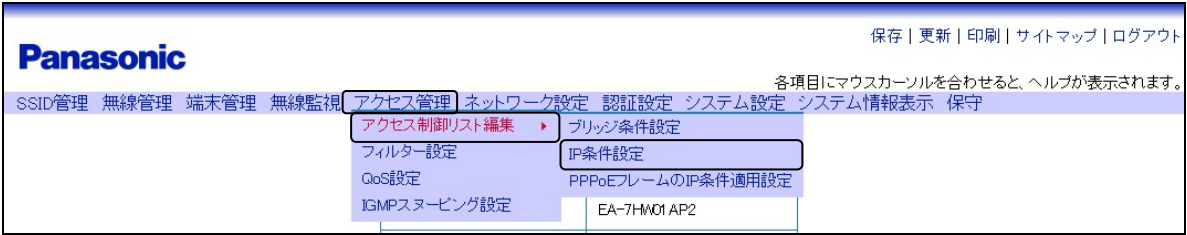



図4.4-10　メニュー（IP 条件設定）

手順2　〔編集〕ボタンをクリックします。

No.	状態	種別	送信元IPアドレス	送信元IPマスク値	送信先IPアドレス	送信先IPマスク値	TOS	プロトコル	送信元ポート	送信先ポート		
1	有効	破棄	192.168.100.254	255.255.255.0	192.168.100.100	255.255.255.0	*	*	*	*	編集	削除
2	無効	透過	*	*	*	*	*	*	*	*	編集	削除

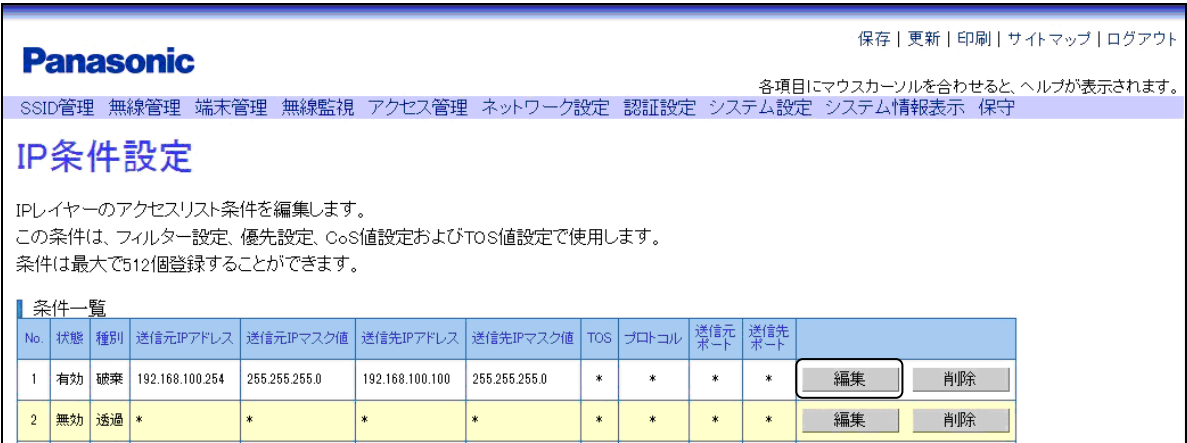



図4.4-11　IP 条件設定

手順3　IP 条件を登録します。

例として、下記内容での設定を示します。

- 実施種別に〔破棄〕を選択（下記条件に合ったものを破棄します。）
- 送信元 IP アドレスは、「192.168.100.254」を入力
- 送信元 IP マスク値は、「255.255.255.0」を入力
- 送信先 IP アドレスは、「192.168.100.100」を入力
- 送信先 IP マスク値は、「255.255.255.0」を入力
- TOS 値、プロトコル番号、送信元ポート番号、送信先ポート番号は、「*（条件設定なし）」を入力

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

IP条件編集

IP条件番号

条件番号	1

条件内容

項目	設定
実施種別 *4 *5 *6	○透過 ◉破棄
送信元IPアドレス *1	192.168.100.254 (xxx.xxx.xxx.xxx [xxx=0～255])
送信元IPマスク値 *1 *3	255.255.255.0 (xxx.xxx.xxx.xxx [xxx=0～255])
送信先IPアドレス *1	192.168.100.100 (xxx.xxx.xxx.xxx [xxx=0～255])
送信先IPマスク値 *1 *3	255.255.255.0 (xxx.xxx.xxx.xxx [xxx=0～255])
TOS *1 *2	* (0～63)
プロトコル番号 *1	* (0～255)
送信元ポート番号 *1 *2	* (0～65535)
送信先ポート番号 *1 *2	* (0～65535)

図4.4-12 IP 条件編集

手順4　画面最下部の〔設定〕ボタンをクリックします。

手順5　〔アクセス管理〕　→　〔フィルター設定〕を選択します。

図4.4-13　メニュー（アクセス管理）

手順6　〔フィルター制御（無線 LAN 送信)〕をクリックし、〔フィルター制御（無線 LAN 送信)〕選択で〔IP 条件〕をクリックします。

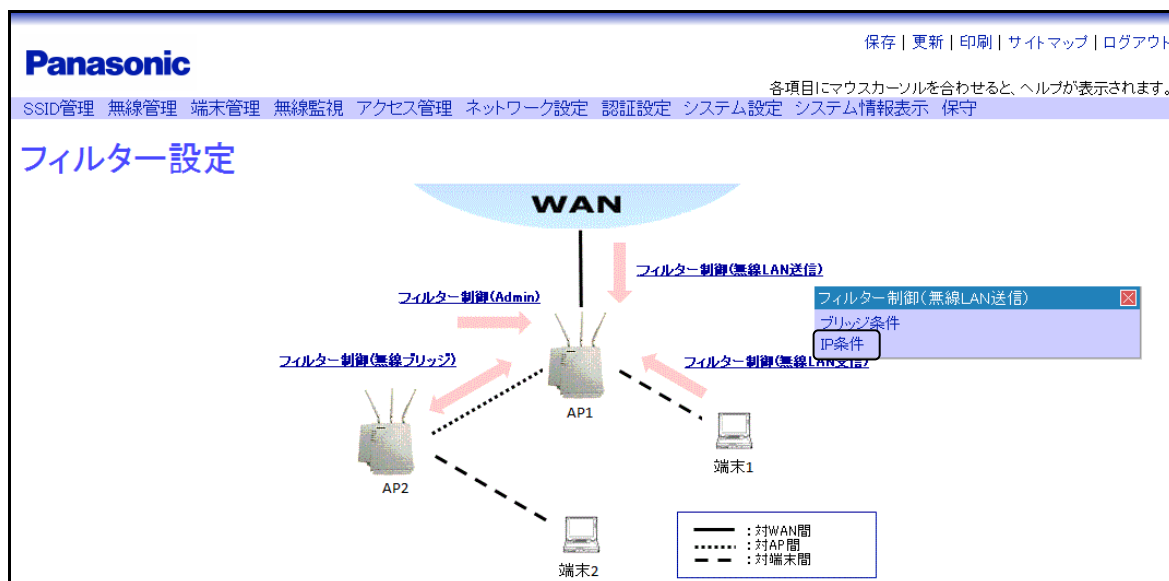



図4.4-14　　フィルター設定(屋内用無線 LAN アクセスポイント)

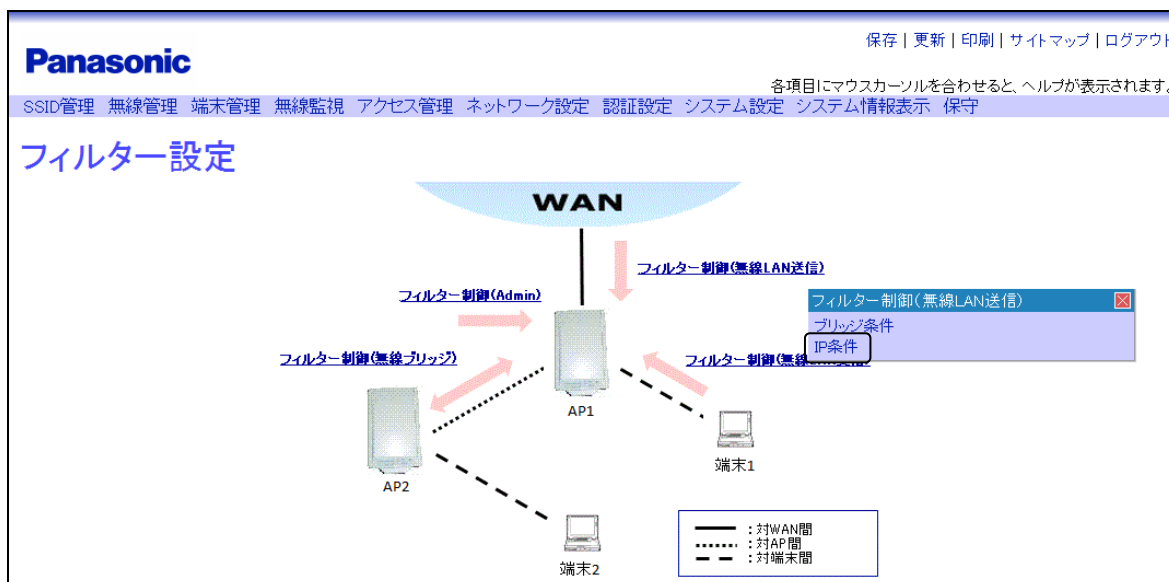



図4.4-15　　フィルター設定(屋外用無線 LAN アクセスポイント)

手順7　IP フィルター設定する SSID 番号をドロップダウンリストから選択し、〔表示〕ボタンをクリックします。

図4.4-16　SSID 選択

手順 7 で〔表示〕ボタンをクリックすると、下記画面が表示されます。(図 4.4-17)

No.	種別	送信元IPアドレス	送信元IPマスク値	送信先IPアドレス	送信先IPマスク値	TOS	プロトコル	送信元ポート	送信先ポート	
1	破棄	192.168.100.254	255.255.255.0	192.168.100.100	255.255.255.0	*	*	*	*	削除
2	透過	192.168.100.254	255.255.255.0	192.168.100.1	255.255.255.0	>63	255	<60000	=60000	削除

図4.4-17　登録済みフィルター条件一覧

手順8　IP フィルター条件番号を入力し、〔登録〕ボタンをクリックする。

図4.4-18　IP フィルター条件登録

◆フィルター設定（PPPoE フィルター条件）

例として IP 条件設定を行った後、PPPoE フィルター条件を設定する方法を説明します。
IP 条件設定手順は、「◆フィルター設定（IP フィルター条件）」 の手順 1 ～ 手順 3 を参照ください。

手順1　〔アクセス管理〕 → 〔アクセス制御リスト編集〕 → 〔PPPoE フレームの IP 条件適用設定〕を選択します。

図4.4-19　メニュー（PPPoE フレームの IP 条件適用設定）

手順2　〔PPPoE フレームの IP 条件適用設定〕をクリックします。

図4.4-20　PPPoE フレームの IP 条件適用設定

手順3　PPPoE フレームの IP 条件適用設定を行う。

例として、下記内容での設定を示します。

・ SSID 番号〔1〕を選択
・ IP 条件を適用する（〔適用させる〕を選択）

図4.4-21　PPPoE フレームの IP 条件適用設定

PPPoE フレームの無線ブリッジ用アクセスフィルタ設定は、〔PPPoE フレームの VLAN-ID 条件適用設定〕にて行います。（図 4.4-22）

図4.4-22　PPPoE フレームの VLAN-ID 条件適用設定（無線ブリッジ条件）

手順4　画面最下部の〔設定〕ボタンをクリックします。

4.5　無線ブリッジ

無線ブリッジ機能を利用して、無線 LAN アクセスポイント同士を無線多段接続することで、無線 LAN エリアを拡充できます。無線ブリッジ接続した無線 LAN アクセスポイントは、Ethernet ケーブルで直接接続した場合と同様に機能します。
中継接続する場合、被接続側の無線 LAN アクセスポイントをサーバーAP、接続を行う無線 LAN アクセスポイントをクライアント AP として設定します。サーバーAP1 台の無線インターフェースごとに最大 8 台（8 分岐）のクライアント AP を接続することが可能です。段数についての制限はありません。
また、無線 LAN アクセスポイントと無線 LAN 端末間の WMM®（Wi-Fi Multimedia ™ ）による QoS 制御に加えて、無線ブリッジ接続時でも QoS 制御が可能です。

ここでは、下の図に示すような多段接続を行うための設定方法を紹介します。

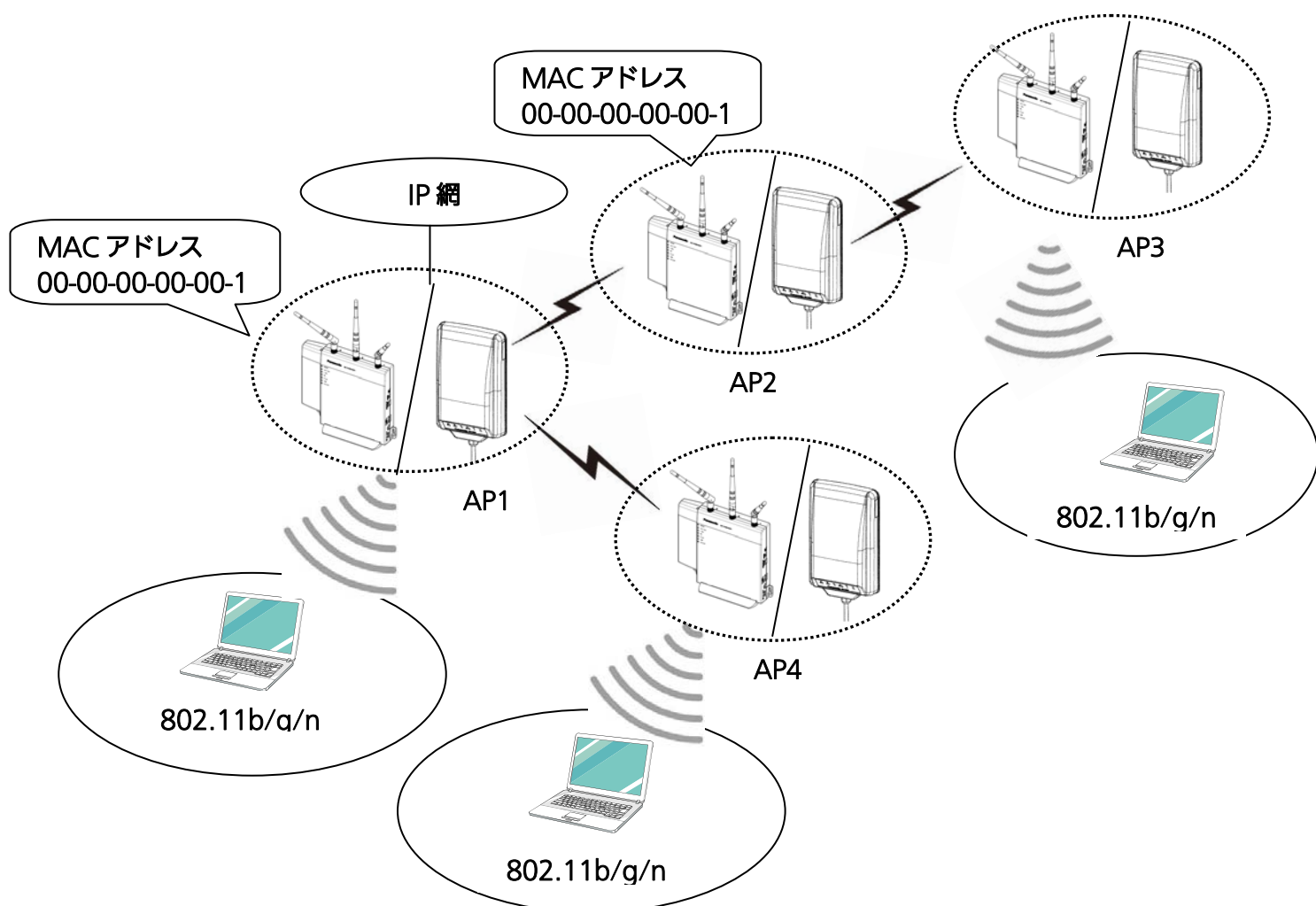



図4.5-1　　構成例（無線ブリッジ）

重要	■ 多段接続になった場合、サーバーAP に各クライアント AP の通信が集約されるので、スループットを考慮してネットワークを構築してください。 ■ クライアント AP のチャネル制御が〔固定〕の場合は、サーバーAP のチャネルに合わせてください。クライアント AP でチャネル制御が自動の場合は、チャネル設定不要です。 ■ 無線ブリッジを行っている状態で端末を収容するには、「端末接続許可設定」を〔許可〕にする必要があります。

設定手順

◆サーバーAP（AP1）の設定

ここでは2.4GHz帯設定を例に説明します。5GHz帯設定選択時の設定方法も同様です。

手順1　〔無線管理〕　→　〔2.4GHz帯設定〕を選択します。

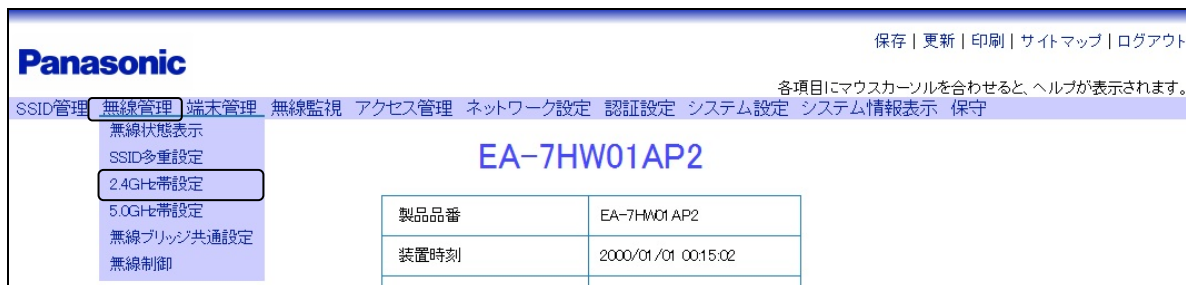



図4.5-2　メニュー（2.4GHz帯設定）

手順2　〔無線ブリッジ〕をクリックします。

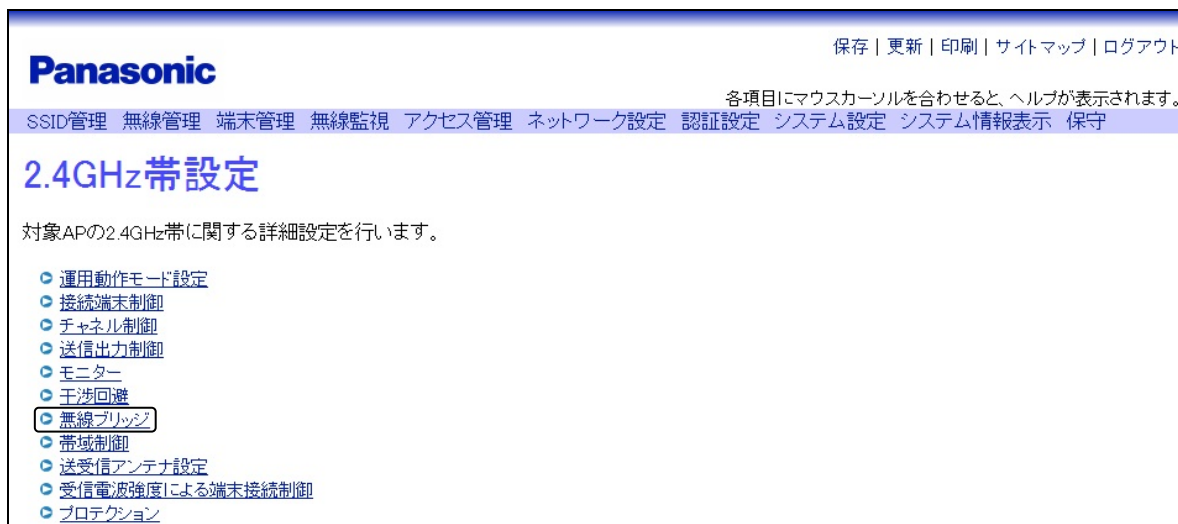



図4.5-3　2.4GHz帯設定

手順3　無線ブリッジの設定を行います。

・ 端末接続許可設定の〔許可〕を選択
・ MAC ブリッジ動作許可設定の〔有効〕を選択

※MAC ブリッジ動作許可設定の設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

無線ブリッジ

項目		設定
ブリッジ接続帯域重み設定		1 (1～10)
端末トラフィック帯域重み設定		1 (1～10)
端末接続許可設定		◉許可 ○禁止
MACブリッジ動作許可設定 (注1)		◉有効 ○無効
MACブリッジ再試行時間設定		0 秒 (0～3600)
AP間RTS/CTS制御設定		○有効 ◉無効
無線IFデータレート	最小値(レガシー)*6	1M
一覧参照 *7	最大値(レガシー)*6	54M
	最小値(11n)*7	15M
	最大値(11n)*7	450M

図4.5-4　無線ブリッジ

手順4　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

◆サーバー／クライアント AP（AP2）の設定
AP2 に対しては、サーバー設定 とクライアント設定 の両方が必要となります。
はじめに、上記 ◆サーバーAP（AP1）の設定 を行い、続いて以下の手順 5 ～ 手順 8 を行います。

手順5 〔無線管理〕 → 〔無線ブリッジ共通設定〕を選択します。

図4.5-5 メニュー（無線ブリッジ共通設定）

手順6 〔無線ブリッジ共通設定〕をクリックします。

図4.5-6 無線ブリッジ共通設定

手順7 MAC ブリッジ共通設定を行います。
- MAC ブリッジクライアント動作設定の〔2.4GHz 帯〕を選択
- MAC ブリッジ事前登録サーバーAP 設定に、AP1 の MAC アドレス「00-00-00-00-00-10」を入力
  （サーバーAP を特定しない場合は、本設定は不要です。）

これらの設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

図4.5-7 MAC ブリッジ共通設定

手順8 上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

◆ クライアント AP（AP3）の設定
AP3 に対しては、クライアント設定のみが必要となります。

手順9　〔無線管理〕　→　〔2.4GHz 帯設定〕、または〔5.0GHz 帯設定〕を選択します。（図 4.5-2）
手順10　〔無線ブリッジ〕をクリックします。（図 4.5-3）
手順11　無線ブリッジの設定を行います。

- 端末接続許可設定の〔許可〕を選択
- MAC ブリッジ動作許可設定の〔無効〕を選択

※クライアント AP（AP3）はサーバーAP 設定は不要なため、MAC ブリッジ動作許可設定を〔無効〕に設定します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

無線ブリッジ

項目		設定
ブリッジ接続帯域重み設定		1 (1〜10)
端末トラフィック帯域重み設定		1 (1〜10)
端末接続許可設定		◉許可 ○禁止
MACブリッジ動作許可設定 (注1)		○有効 ◉無効
MACブリッジ再試行時間設定		0 秒 (0〜3600)
AP間RTS/CTS制御設定		○有効 ◉無効
無線IFデータレート	最小値(レガシー) *6	1M
一覧参照 *7	最大値(レガシー) *6	54M
	最小値(11n) *7	15M
	最大値(11n) *7	450M

図4.5-8　無線ブリッジ

手順12　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

引き続き ◆サーバー／クライアント AP（AP2）の設定 の手順 5 〜 手順 8 を行います。
AP3 のサーバーAP は AP2 となるため、手順 7 にて入力する MAC アドレスは AP2 の MAC アドレス「00-00-00-00-00-11」となります。

◆ クライアント AP（AP4）の設定
AP4 に対しては、クライアント設定のみが必要となります。
◆サーバー／クライアント AP（AP3）の設定 の手順 9 〜 手順 12 を行います。
引き続き◆サーバー／クライアント AP（AP2）の設定 の手順 5 〜 手順 8 を行います。

以上で、無線 LAN アクセスポイント間無線ブリッジ機能の設定は完了です。

4.6　VoIP利用時の各種設定

本装置には、VoIP 利用時の通話品質を維持するための機能が用意されています。ここでは、VoIP 利用時の各種設定方法を紹介します。

4.6.1　通話数制限機能

本装置 には、3 種類の通話数制御機能（コール・アドミッション・コントロール、TSPEC、通信量）が用意されています。

■コール・アドミッション・コントロールによる端末接続数制御

コール・アドミッション・コントロール機能によって、端末接続数に応じて発呼／着呼制限や、非通話端末の切断など呼の管理を行うことも可能です。
コール・アドミッション・コントロール機能では、通信量ではなく、SIP のセッション制御を監視して、呼を管理します。この方式では、即時に通話中／非通話を判断できるため、より効率的な端末接続数制御が可能となります。

表4.6-1　通話数による端末数制御一覧表

閾値	説明
通話開始拒否	通話端末がこの閾値に達した場合、新規の通話は拒否されます。
新規端末拒否	通話端末がこの閾値に達した場合、新規の接続要求端末は拒否されます。
非通話端末切断	通話端末がこの閾値に達した場合、アイドル状態の端末は切断されます。

※無線 LAN アクセスポイントを通過する SIP フレームが暗号化されていなかった場合のみ、監視が可能となります。

設定手順

手順1　〔端末管理〕　→　〔コール・アドミッション・コントロール〕
→　〔コール・アドミッション・コントロール設定〕を選択します。

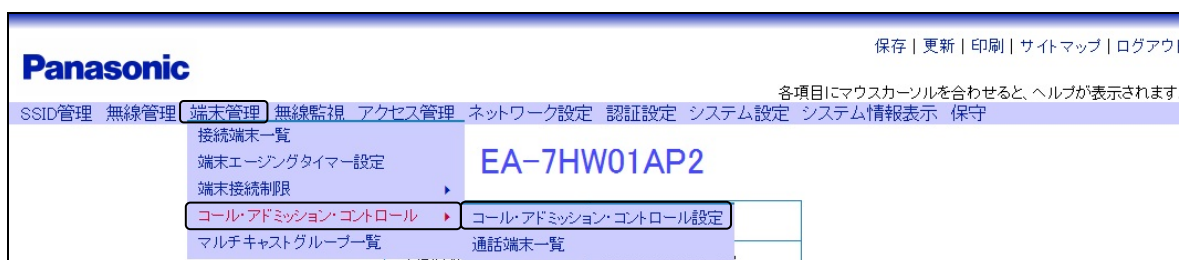



図4.6-1　メニュー（コール・アドミッション・コントロール設定）

手順2　〔コール・アドミッション・コントロール有効／無効〕をクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

コール・アドミッション・コントロール設定

通話端末数に応じて発呼／着呼制限や、非通話端末の切断など呼の管理を行います。

- コール・アドミッション・コントロール有効／無効
- セッション情報エージング時間
- コール・アドミッション・コントロール詳細設定(2.4GHz帯)
- コール・アドミッション・コントロール詳細設定(5.0GHz帯)
- 通話開始拒否方法

図4.6-2　コール・アドミッション・コントロール設定

手順3　コール・アドミッション・コントロールを〔有効〕にします。

図4.6-3　コール・アドミッション・コントロール有効／無効

手順4　不要なセッション情報と判断するまでのエージング時間を設定します。

例として、「20 秒」を設定します。

図4.6-4　セッション情報エージング時間

手順5　3 種類の通話接続制限の方法ごとの閾値を設定することで、コントロールの方法を指定します。

例として、2.4GHz 帯に下記設定を行います。

・　新規通話を拒否する閾値として、「200 台」
・　新規接続要求を拒否する閾値として、「215 台」
・　アイドル状態の端末を切断する閾値として、「230 台」

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

コール･アドミッション･コントロール詳細設定(2.4GHz帯)

通話開始拒否	通話端末が 200 台に達した場合に、新規の通話を拒否する。*2
新規端末拒否	通話端末が 215 台に達した場合に、新規の接続要求端末を拒否する。*2
非通話端末切断	通話端末が 230 台に達した場合に、アイドル状態の端末を切断する。*2

*2　1AP当り端末台数(0(＝無制限)/1～320)

図4.6-5　コール・アドミッション・コントロール詳細設定（2.4GHz 帯）

手順6　新規の通話拒否を設定している場合は、拒否の方法を指定します。

例として、下記内容での設定を示します。

- 発呼制限方法として、〔通話拒否〕を選択
- 着呼制限方法として、〔端末切断〕を選択

図4.6-6　通話開始拒否方法

手順7　画面最下部の〔設定〕ボタンを押し、設定を反映させせます。

■TSPEC による通話数制御の設定

TSPEC とは、AC_VO（音声）、AC_VI（映像）に対する無線区間の品質確保を目的としたアドミッション制御機能です。TSPEC では、送信したいトラフィックの伝送条件をあらかじめ無線 LAN アクセスポイントに伝え、利用可能な帯域を予約することで、通信品質を確保します。TSPEC 対応端末をご利用になる場合は、この機能を有効にすることをおすすめします。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図4.6-7　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

図4.6-8　SSID 設定

手順3　対象となる SSID の〔編集〕ボタンをクリックします。

図4.6-9　SSID 一覧

手順4　〔QoS〕をクリックします。

図4.6-10　SSID 編集

手順5　TSPEC に関するパラメーターを設定します。

例として、下記内容での設定を示します。

- 当該 SSID を〔WMM 規格に沿った QoS 制御〕に設定
- TSPEC アドミッション受付の音声と映像の両方を〔有効〕に設定

図4.6-11　QoS

手順6　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

■通信量による端末接続制御

通信量による端末接続制御機能では、端末単位に通信量（伝送パケット数）を監視し、通信量が閾値を上回る場合に通信中であるとみなし、通信端末数に基づいた接続制限を行います。

表4.6-2　通信端末数による通信数制御一覧表

閾値	説明
接続最大端末数	通信端末数がこの閾値に達した場合、新たな接続要求端末をすべて拒否します。
非通信端末切断	通信端末数がこの閾値に達した場合、アイドル状態のすべての端末を切断します。
通信端末切断	通信端末数がこの閾値に達した場合、通信中の端末を含めすべての端末を切断します。

ここでは、VoIP 端末の接続を優先したい場合の設定方法を紹介します。データ端末用の SSID（DATA）に対して、次のような設定を行います。

- 通信端末が 18 台に達した場合に、新たな接続要求端末を拒否する。
- 通信端末が 20 台に達した場合に、アイドル状態の端末を切断する。
- 通信端末が 22 台に達した場合に、通信している全端末を切断する。

たとえば、VOICE と DATA を介した通信端末数が合わせて 18 台に達すると、DATA を介した新たな端末の接続は拒否されます。さらに、VOICE を介して新たな VoIP 端末 2 台が通信し、通信端末数が 20 台に達すると、DATA を介して接続している端末の中で、アイドル状態の端末が切断されます。最終的に、総端末数が 22 台に達すると、DATA を介して通信をしている全端末が切断されて、VOICE を介して接続しようとしている VoIP 端末に十分な帯域が確保されます。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

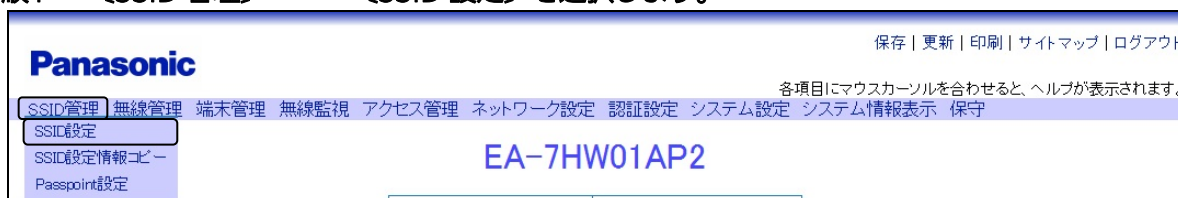



図4.6-12　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

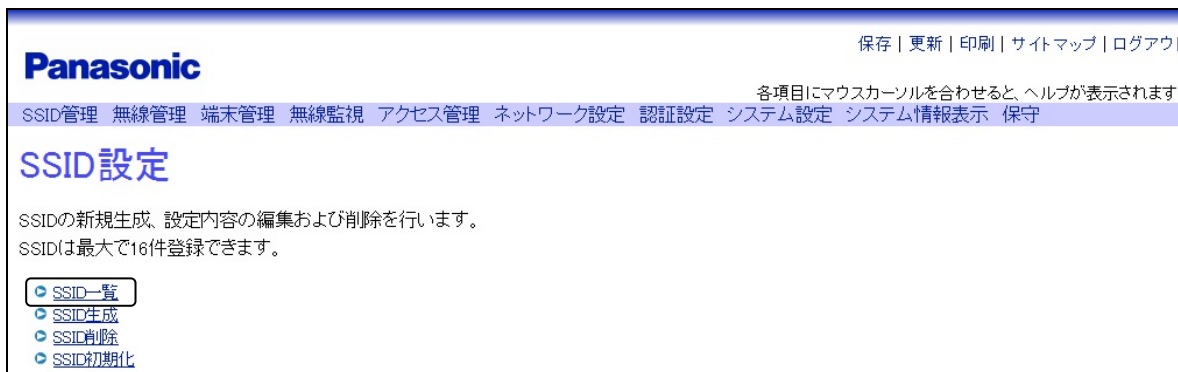



図4.6-13　SSID 設定

手順3　対象となるSSIDの〔編集〕ボタンをクリックします。

図4.6-14　SSID一覧

手順4　通信端末数による端末接続制御をクリックします。

図4.6-15　SSID編集

手順5　通信端末数による端末接続制御設定を行います。

例として、下記内容での設定を示します。

- 端末接続制御で〔使用する〕を選択
- 使用無線インターフェースは、〔2.4GHz 帯〕を選択
- 新規接続を拒否する閾値に「18 台」を設定
- アイドル状態の端末を切断する閾値に「20 台」を設定
- 通信中の全端末を切断する閾値に「22 台」を設定

図4.6-16　通信中端末数による端末接続制御

手順6　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

4.6.2　代理ARP応答

本装置は、端末の ARP 問い合わせに対して、代理 ARP を行うことができます。これによって省電力モードの端末が無駄に起動する必要がなくなるため、帯域と電力の両方を節約できます。
代理 ARP 応答動作には、未学習端末宛フレーム透過と未学習端末宛フレーム破棄の 2 種類があります。

未学習端末宛てフレーム破棄にすると、無線 LAN アクセスポイントで ARP テーブルに登録がない IP アドレスへの ARP 要求（無線 LAN 端末ではない装置への ARP 要求）を遮断するため、不要なフレームを無線上に送信せず、無線 LAN 端末の電力をより節約することができます。
ただし、この場合、無線 LAN 端末宛の未学習 IP の ARP 要求はすべて遮断されるので、無線 LAN 端末やネットワーク内のほかの装置の ARP テーブルエージングタイマーを長く設定するなどして、無線 LAN アクセスポイントで学習した無線 LAN 端末の ARP テーブルがエージングされる前に更新されるように、運用してください。
本装置の代理 ARP 応答は IPv4/v6 の両方に対応しており、下記で説明する設定は IPv4/v6 で共通です。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

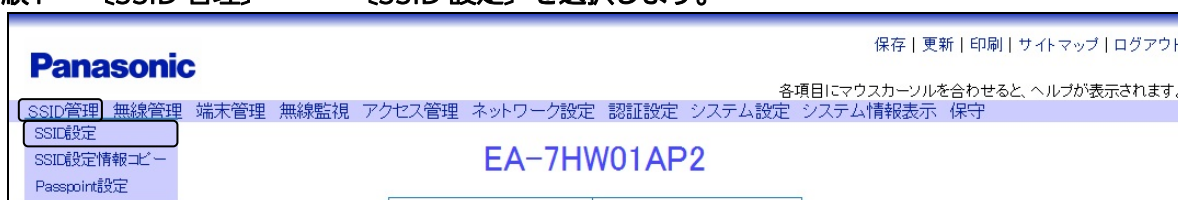



図4.6-17　SSID 設定

手順2　〔SSID 一覧〕をクリックします。

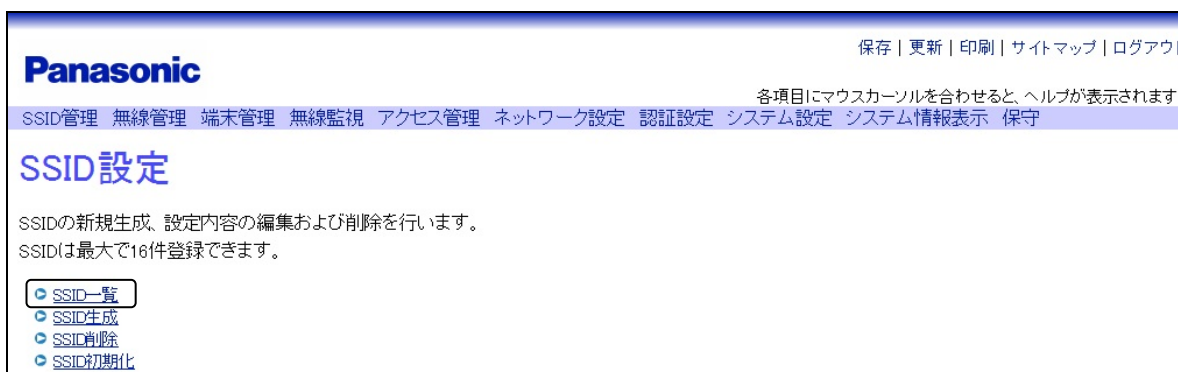



図4.6-18　SSID 設定

手順3　対象となる SSID の〔編集〕ボタンをクリックします。

図4.6-19　SSID 一覧

手順4　〔代理 ARP 応答〕をクリックします。

図4.6-20　SSID 編集

手順5　代理 ARP 応答動作を設定します。

例として、下記内容での設定を示します。

- 代理 ARP 応答動作を〔未学習端末宛てフレーム破棄〕に設定
- 代理応答端末エージングタイマーを「3600 秒」に設定

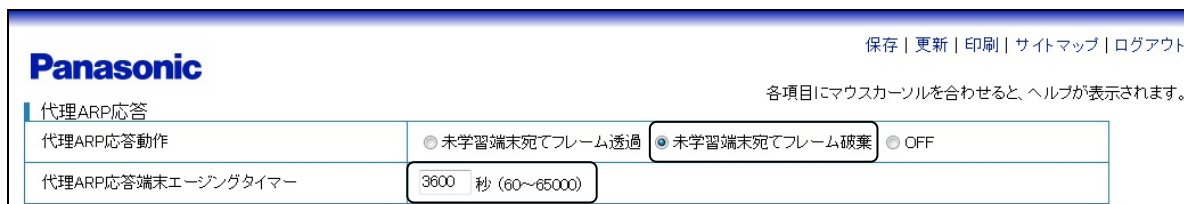



図4.6-21　代理 ARP 応答

手順6　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

4.6.3　VoIP/Video自動優先割り当て

SIP パケットのスヌーピングを行い、VoIP、および Video データの優先度を自動的に割り当てます。

設定手順

手順1　〔アクセス管理〕　→　〔QoS 設定〕を選択します。

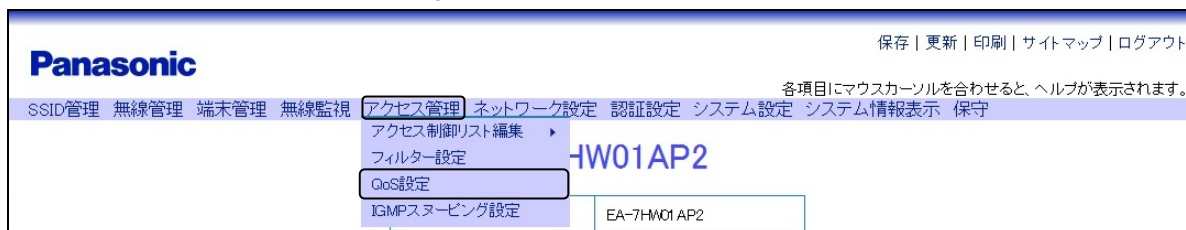



図4.6-22　メニュー（QoS 設定）

手順2　〔優先度自動設定〕をクリックします。

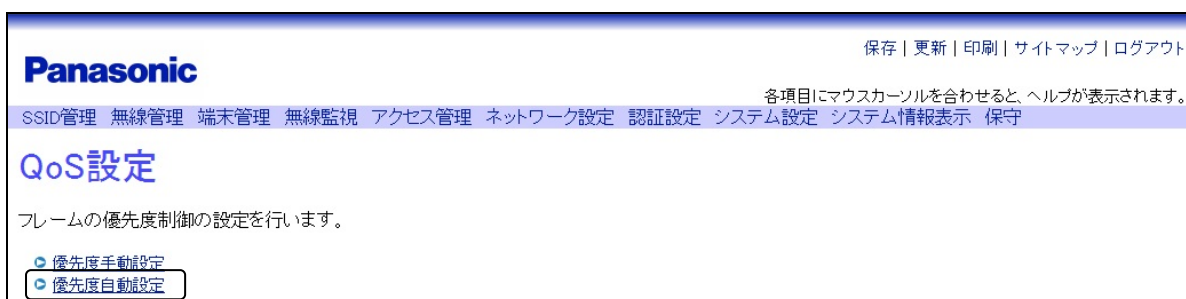



図4.6-23　QoS 設定

手順3　音声フレーム優先制御を〔有効〕にします。

図4.6-24　優先度自動設定

手順4　画面最下部〔設定〕ボタンを押し、設定を反映させせます。

4.7　サービス品質向上機能

4.7.1　5GHz帯への端末誘導設定

2.4GHz 帯は多くの機器が混雑しているため、本装置では、5GHz 帯に対応している端末に対しては 2.4GHz 帯での接続を行わず、5GHz 帯での接続を促す機能を持ちます。
また、当機能は SSID 単位で設定が行えます。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

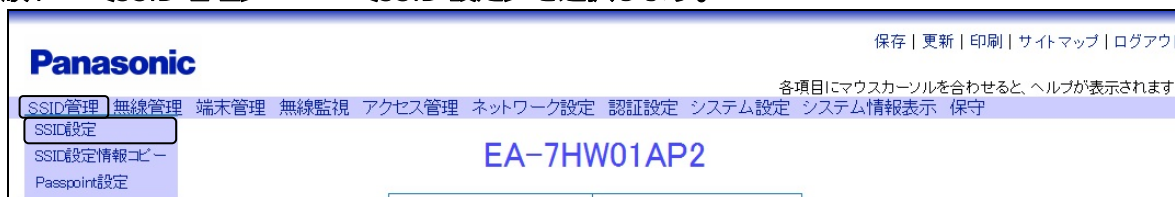



図4.7-1　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

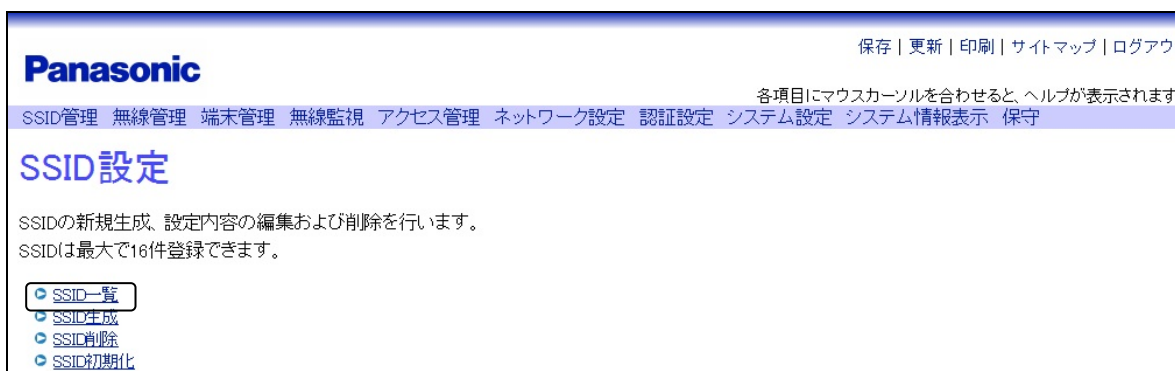
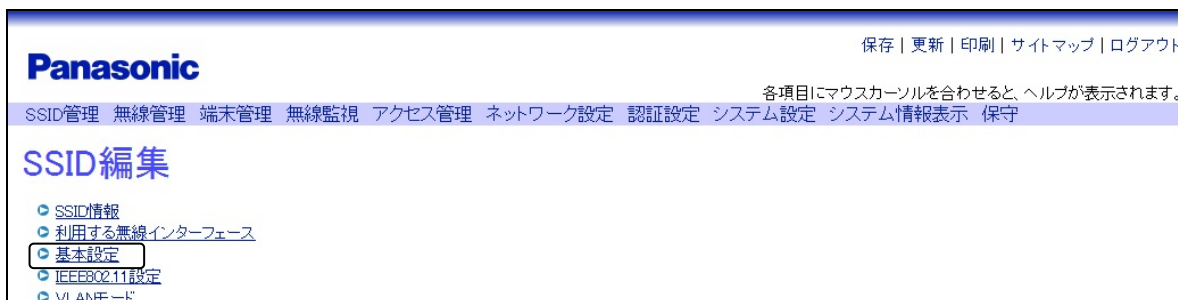



図4.7-2　SSID 設定

手順3　対象となる SSID の〔編集〕ボタンをクリックします。

図4.7-3　SSID 一覧

手順4　〔基本設定〕をクリックします。

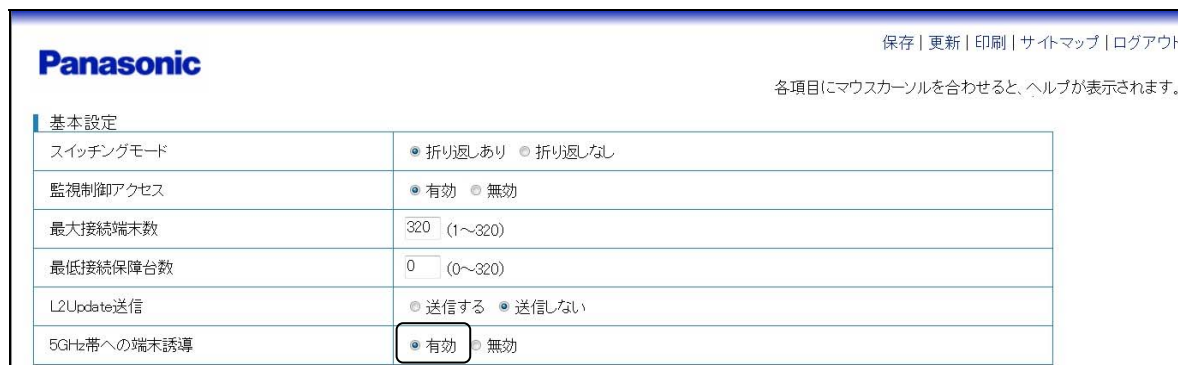



図4.7-4　SSID 編集

手順5　5GHz 帯への端末誘導 を〔有効〕にします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

基本設定

スイッチングモード	◉ 折り返しあり ○ 折り返しなし
監視制御アクセス	◉ 有効 ○ 無効
最大接続端末数	320 (1～320)
最低接続保障台数	0 (0～320)
L2Update送信	○ 送信する ◉ 送信しない
5GHz帯への端末誘導	◉ 有効 ○ 無効

図4.7-5　基本設定

手順6　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

4.7.2　小セル化（ビーコンレートの指定）

ビーコンの送信レートを上げることで、ビーコン検出可能エリアを安定した通信ができるエリアに絞り込み、電界が不安定なエリアの端末を接続させなくする（小セル化を実現する）ことで、通信サービスの品質を向上させます。

図4.7-6は、ビーコンレートを6Mbpsに指定することで、検出不可エリアの端末を接続させなくしています。

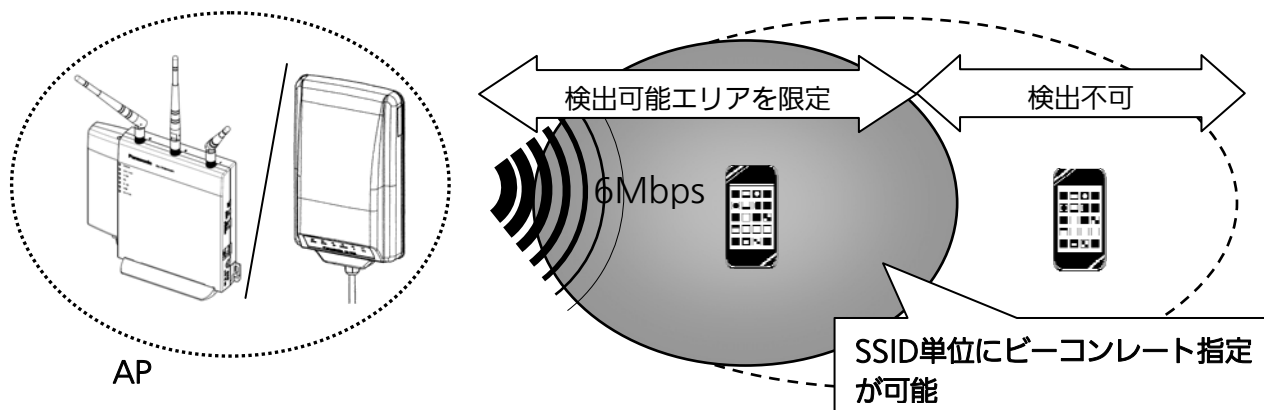



図4.7-6　ビーコンレート指定例

設定手順

手順1　〔無線管理〕　→　〔SSID 多重設定〕を選択します。

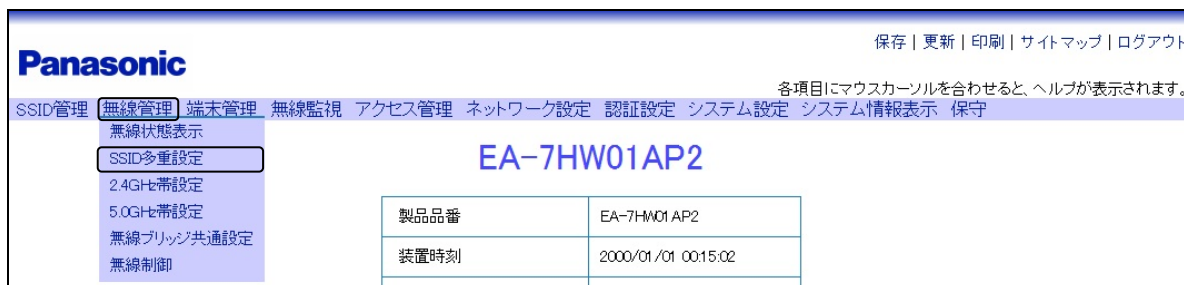



図4.7-7　メニュー（SSID 多重設定）

手順2　対象となる SSID の〔編集〕ボタンをクリックします。

例として、SSID：1 の編集を行います。

登録番号 *1	SSID動作	登録SSID番号	SSID名	SSID値	
1	有効	1	SalesGroup	SALES	編集
2	無効				編集

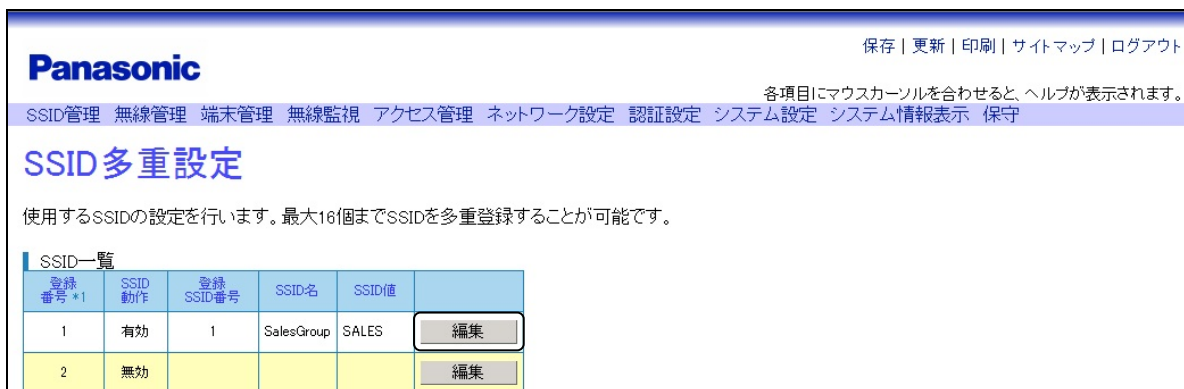



図4.7-8　SSID 多重設定

手順3　〔2.4GHz 帯設定〕、または〔5.0GHz 帯設定〕をクリックし、ビーコンレート制御の設定を行います。

例として、2.4GHz 帯設定を選択し、設定を行います。

・ ビーコンレート制御：〔有効〕を選択
・ ビーコンレート：〔6M〕を選択

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

2.4GHz帯設定

送信制御	ブロードキャスト制御	○送信遮断を行う ◉送信遮断を行わない
	マルチキャスト制御	○送信遮断を行う ◉送信遮断を行わない
データレート	制御モード	○固定 ◉自動
一覧参照 *3	最小値(レガシー) *2	1M
	最大値(レガシー) *2	54M
	最小値(11n) *3	15M
	最大値(11n) *3	450M
	ブロードキャストレート制御	○有効 ◉無効
	ブロードキャストレート *4	24M
	マルチキャストレート制御	○有効 ◉無効
	マルチキャストレート *4	24M
	ビーコンレート制御	◉有効 ○無効
	ビーコンレート *4	6M
帯域比率		1 (1～10)

図4.7-9　2.4GHz 帯設定（SSID 多重設定）

手順4　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

4.7.3　同時接続端末数制御

無線 LAN アクセスポイントに、接続可能な最大端末数を設定することで、通信品質の極端な低下を回避できます。また、データ受信時に端末間の電界レベルを測定し、最大接続端末数に対する接続端末数の比率が設定した値に達した場合、一定の電界レベル（設定値）以下の端末からの接続を拒否することで、接続中の端末の通信品質を保つことも可能です。

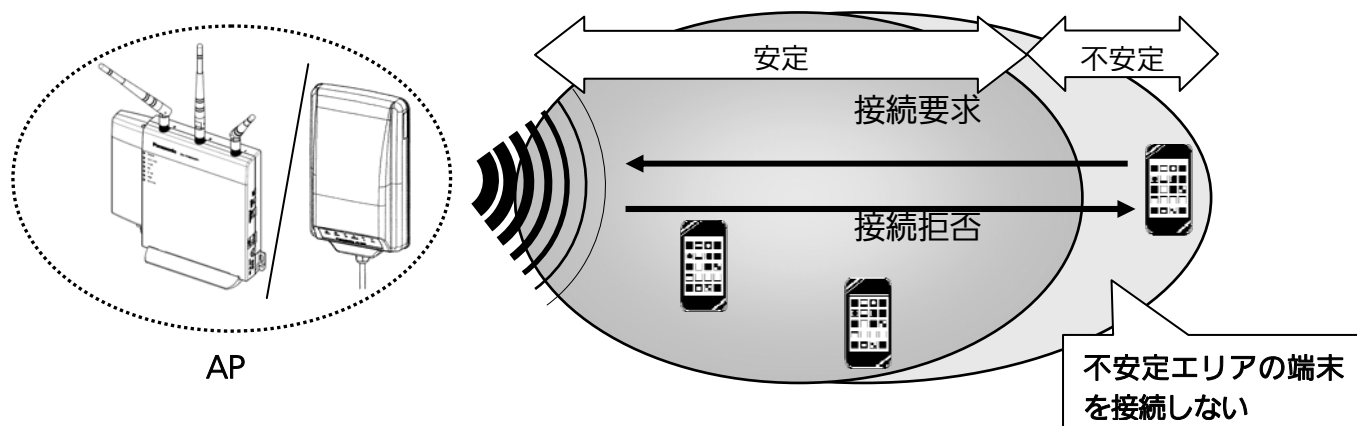



図4.7-10　　受信電波強度による端末接続制御例

ここでは、2.4GHz 帯設定を例に、最大接続数を固定で制限する方法と受信電波強度で端末接続数を制御する方法を紹介します。

設定手順

◆最大接続端末数設定

手順1　〔無線管理〕　→　〔2.4GHz 帯設定〕を選択します。

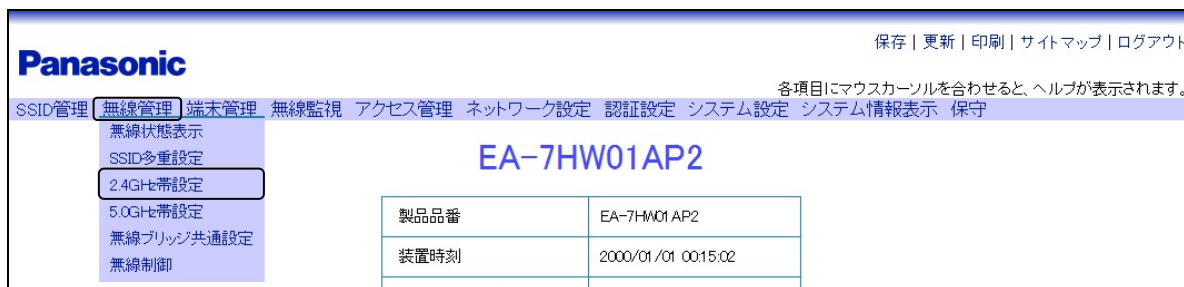



図4.7-11　　メニュー（2.4GHz 帯設定）

手順2　〔接続端末制御〕をクリックします。

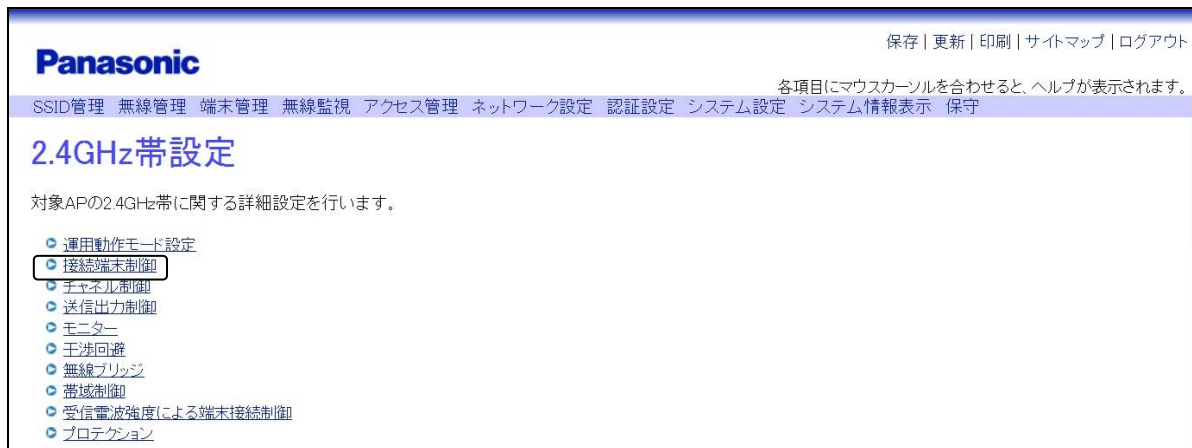



図4.7-12　2.4GHz 帯設定

手順3　最大接続端末数を設定します。

※　この設定変更では、設定した情報を有効にさせるために保存とリセットが必要となります。

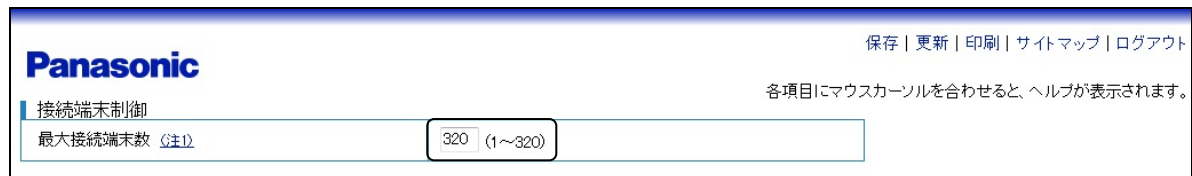



図4.7-13　接続端末制御

手順4　画面最下部〔設定〕ボタンを押し、設定を反映させます。

設定手順

◆受信電波強度による端末接続制御

手順1　〔無線管理〕　→　〔2.4GHz 帯設定〕を選択します。

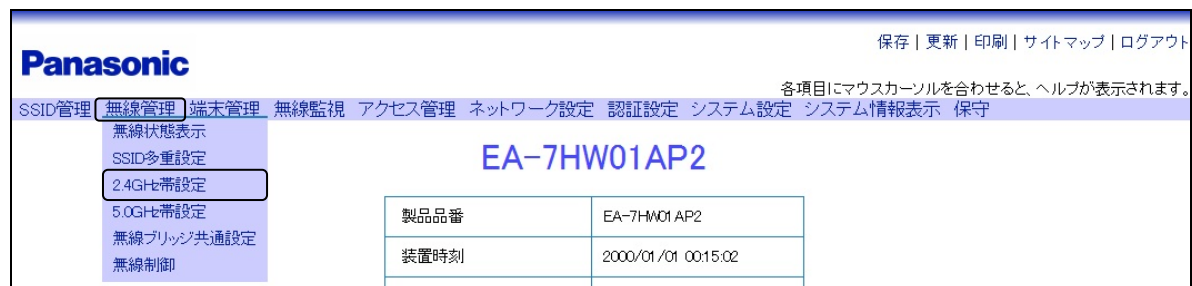



図4.7-14　メニュー（2.4GHz 帯設定）

手順2　〔受信電波強度による端末接続制御〕をクリックします。

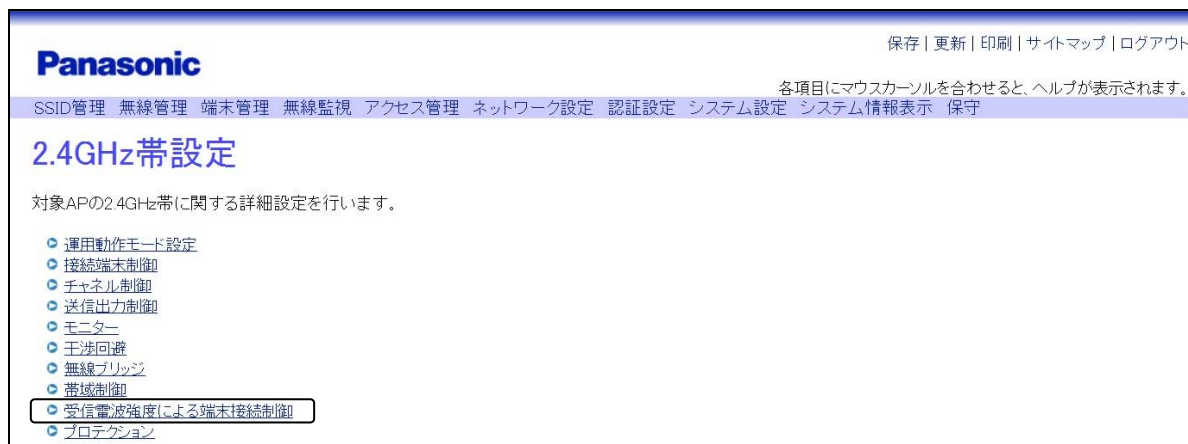



図4.7-15　2.4GHz 帯設定

手順3　受信電波強度による端末接続制御の設定を行います。

例として、下記内容での設定を示します。

- 端末接続制御の〔有効〕を選択
- 端末接続制御の有効化割合に「80」を入力

上記設定では、最大接続端末数に対する接続端末数の比率が 80%以上となると、端末接続制御が動作します。

図4.7-16　受信電波強度による端末接続制御

手順4　画面最下部〔設定〕ボタンを押し、設定を反映させます。

4.7.4　最低接続保証台数制御

本装置では、最大接続端末数に加えて、最低接続保証台数を設定することができます。最低接続保証台数はSSID 単位で管理します。
各 SSID に対する最低接続保証台数の合計が無線インターフェースの最大接続端末数を超える場合、設定した台数分すべての端末接続が保証されなくなりますので注意してください。

例）使用する無線インターフェースの最大接続端末数：5 台
　　最低接続保証台数を SSID1：2 台、SSID2：3 台とし、接続中端末は SSID1、2 共に 2 台とします。

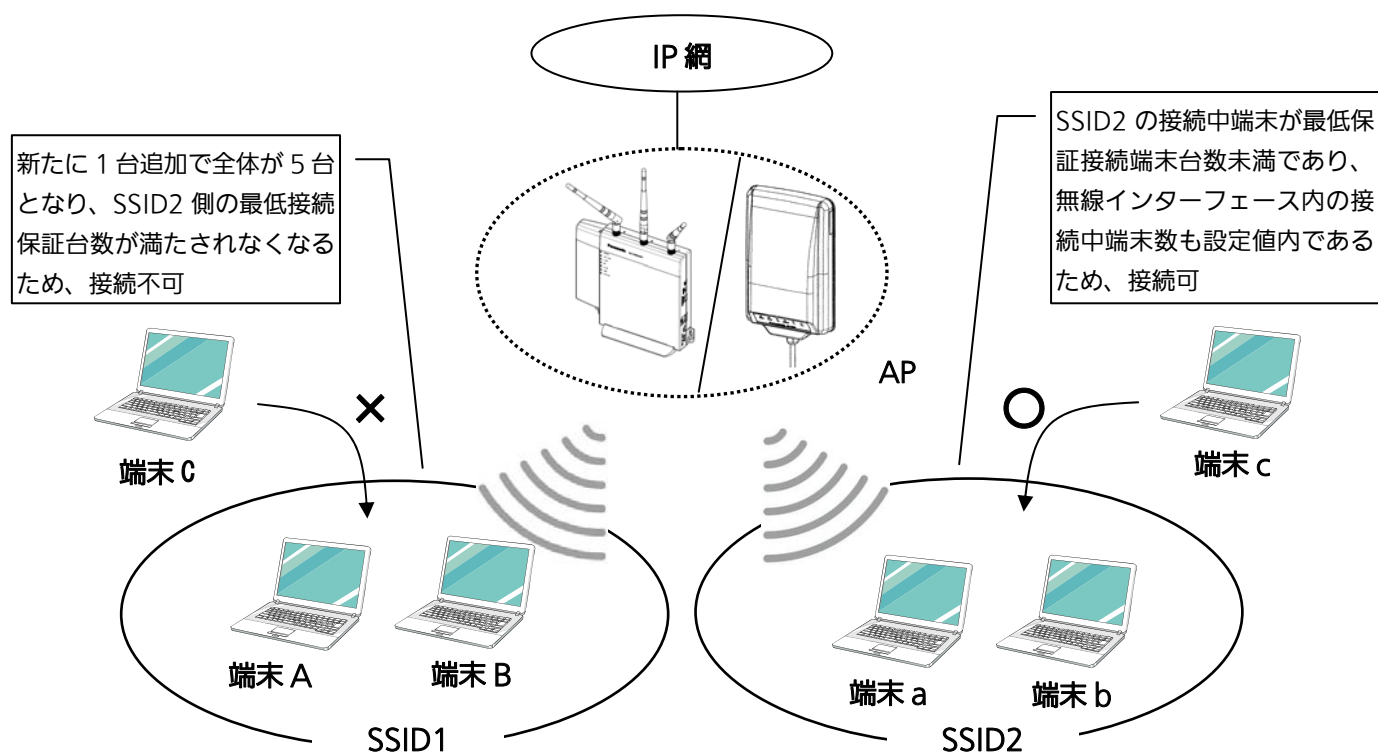



図4.7-17　　最低接続端末数制御例

設定手順

無線インターフェースの最大接続端末数は、前項 にて設定済みとして説明します。

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

図4.7-18　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

図4.7-19　SSID 設定

手順3　対象となる SSID の〔編集〕ボタンをクリックします。

例として、SSID1 の設定を行います。

SSID一覧

SSID番号	SSID名	SSID値（先頭の20文字を表示します）	VLANモード	SSID VLAN-ID	スイッチングモード設定	
1	SalesGroup		OFF	1	折り返しあり	編集

図4.7-20　SSID 一覧

手順4　〔基本設定〕をクリックします。

図4.7-21　SSID 編集

手順5　最低接続保証台数に「2」を入力します。

図4.7-22　最低接続保障台数

手順6　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

4.7.5　IGMPスヌーピング

IGMP スヌーピング機能は、上位ルーターと端末間の IGMP トラフィックを覗き見（スヌーピング）し、マルチキャストが存在しない SSID に対するトラフィックを抑制することで、無駄なマルチキャストトラフィックを削減します。この機能によって、無線 LAN の通信品質が維持されます。
IGMP スヌーピング機能は、以下の 2 つの機能から構成されています。

- マルチキャストグループ管理機能
- マルチキャストフレームフィルタリング機能

IGMP スヌーピング機能を有効にすると、本装置 は無線 LAN 端末から送信される IGMP トラフィック（Membership Report）で通知されるマルチキャストグループを学習し、各 SSID 配下に存在するマルチキャストグループの管理を開始します。
また、あるマルチキャストグループに属する SSID 配下の無線 LAN 端末から、そのグループに該当する Membership Report を一定時間受信しない場合、その SSID をグループから除外します。この時間をグループエージングタイマーと呼びます。
ここでは、IGMP スヌーピング機能を有効にするための方法を紹介します。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

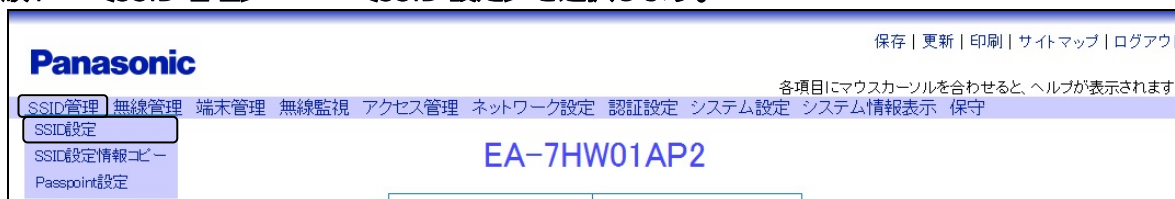



図4.7-23　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

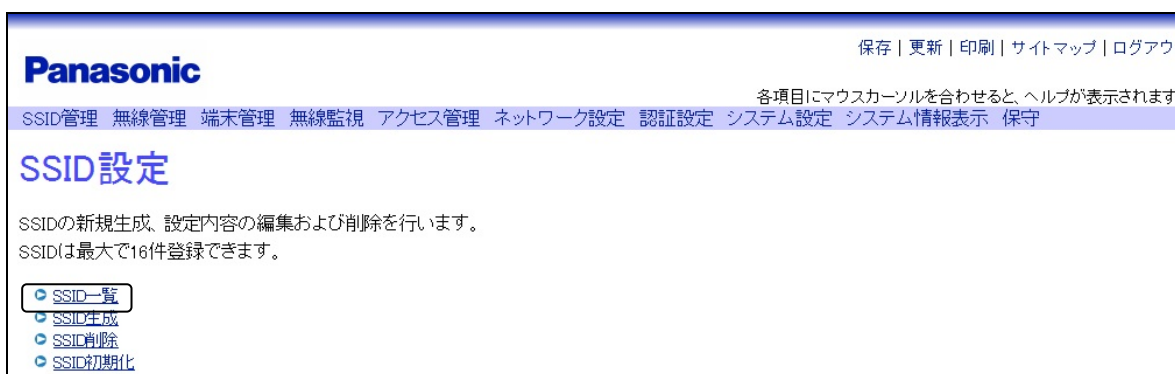



図4.7-24　SSID 設定

手順3　対象となる SSID の〔編集〕ボタンをクリックします。

図4.7-25　SSID 一覧

手順4　〔IGMP スヌーピング〕をクリックします。

図4.7-26　SSID 編集

手順5　IGMP スヌーピングを〔有効〕にします。

図4.7-27　IGMP スヌーピング

手順6　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

※ グループエージングタイマー設定を行う場合は、下記をご参照ください。
〔アクセス管理〕 → 〔IGMP スヌーピング〕を選択します。

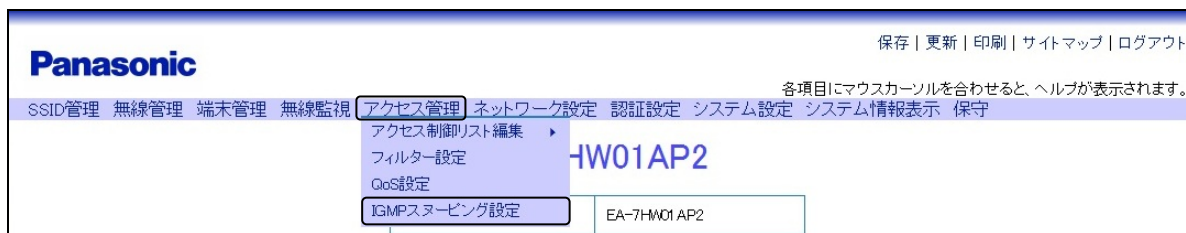



図4.7-28 メニュー（IGMP スヌーピング設定）

〔IGMP スヌーピング設定〕画面で、グループエージングタイマー設定します。
〔グループエージングタイマー〕は〔Query 間隔〕、〔Query 応答時間〕、〔Robustness 値〕を入力することで算出して表示されます。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守

IGMPスヌーピング設定

IGMPスヌーピングの設定によりマルチキャストグループの管理を行います。

グループエージングタイマー設定

Query 間隔	125 秒 (1～3600)
Query 応答間隔	10 秒 (1～25)
Robustness値	2 回 (1～10)
グループエージングタイマー *1	260 秒 (2～18000)

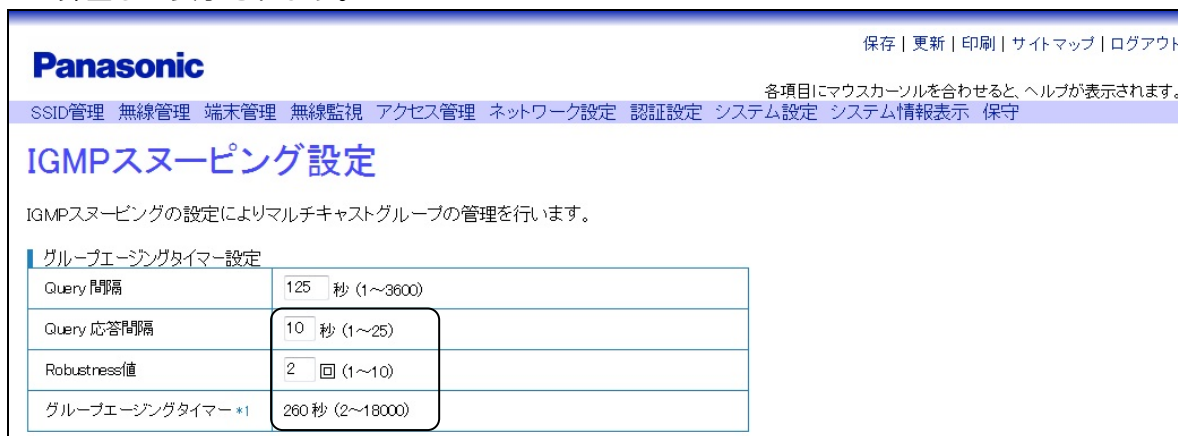



図4.7-29 IGMP スヌーピング設定（グループエージングタイマ設定）

手順7 画面最下部〔設定〕ボタンを押し、設定を反映させます。

■学習状況の確認

マルチキャストグループの学習状況に従って、マルチキャストフレームはフィルタリングされます。
たとえば、マルチキャストフレームの転送先 SSID の IGMP スヌーピング機能が有効の場合で、転送先 SSID に該当するマルチキャストグループが存在しなければ、そのフレームはフィルタリング機能によって不透過となります。ただし、同じマルチキャストアドレスの学習がほかに存在しない場合、そのフレームは転送されます。
マルチキャストグループの学習状況を確認にするための方法を紹介します。

操作手順

手順1 〔端末管理〕 → 〔マルチキャストグループ一覧〕を選択します。

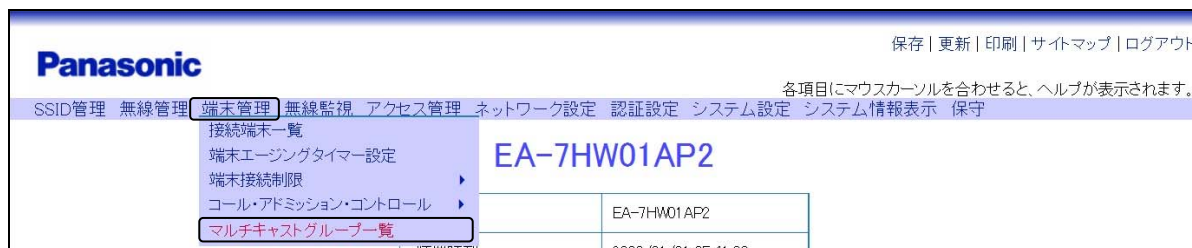
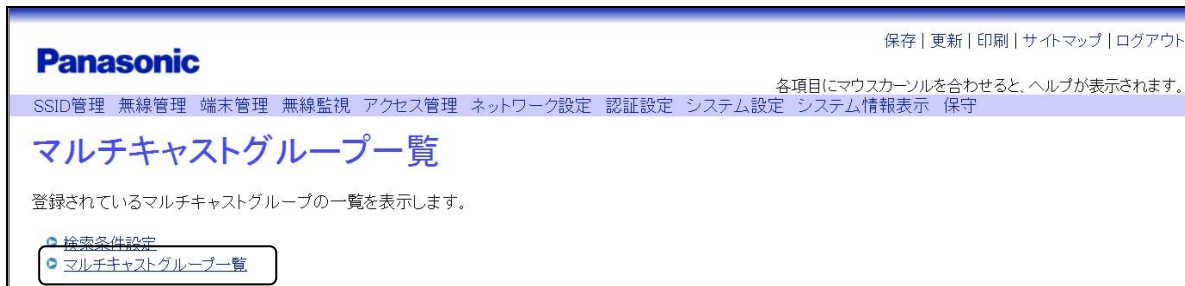



図4.7-30 メニュー（端末管理）

手順2　〔マルチキャストグループ一覧〕をクリックします。

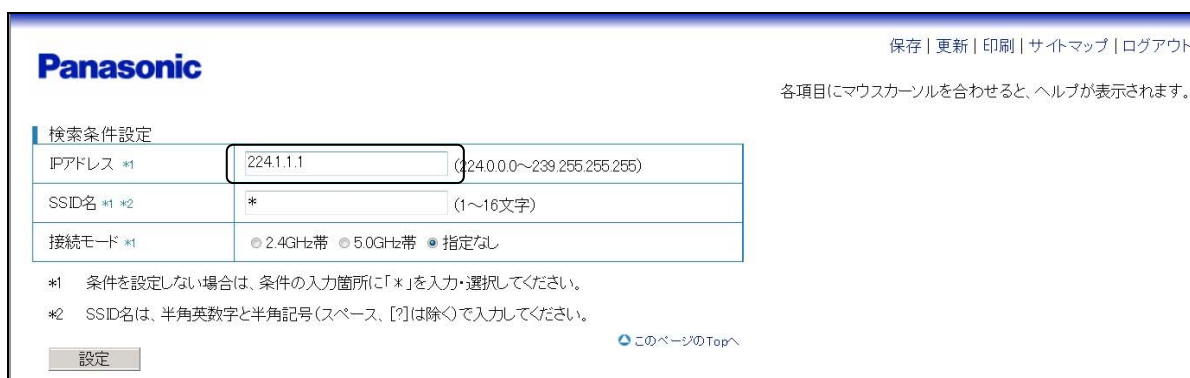



図4.7-31　マルチキャストグループ一覧

手順3　検索するマルチキャストグループの条件を入力します。

例として、下記内容での設定を示します。

・ IP アドレスに「224.1.1.1」を入力

図4.7-32　マルチキャストグループ検索条件設定

手順4　〔設定〕ボタンを押すと、検索したマルチキャストグループ一覧を確認できます。

4.7.6　Passpoint機能

Passpoint は、Wi-Fi Alliance によって策定された規格「Hotspot 2.0」のサービス名です。 本製品の Passpoint は、以下の機能を提供します。(Wi-Fi Alliance フェーズ 1 に対応しています)

- ネットワークの発見および選択
  → ユーザーが操作しなくても端末がネットワークを発見し、
  自動的に接続する機能を提供します。

- シームレスなネットワークアクセス
  → ブラウザでのサインオンや、ユーザーによるパスワードの入力を必要とせず、
  SIM カードやユーザー名／パスワード、証明書に基づく EAP 認証を行うことにより
  シームレスなネットワークアクセスを提供します。

- 安全な認証および接続
  →セルラーネットワークに匹敵する安全性を提供します。

ここでは、Passpoint 機能を有効にするための方法を紹介します。

設定手順

手順1　〔SSID 管理〕　→　〔Passpoint 設定〕を選択します。

図4.7-33　メニュー（Passpoint 設定）

手順2　対象となる SSID の〔編集〕ボタンをクリックします。

登録番号 *1	SSID動作	登録SSID番号	SSID名	SSID値	
1	有効	1	SalesGroup	SALES	編集

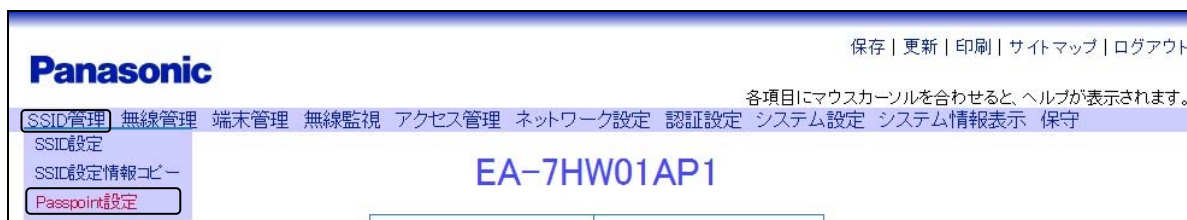



図4.7-34　Passpoint 設定一覧（SSID 一覧）

手順3　〔Passpoint 設定〕をクリックします。

図4.7-35　Passpoint 編集

手順4　Passpoint 設定を〔有効〕にします。

Passpoint 機能を、〔有効〕に機能させるためには、あらかじめ〔SSID 編集〕画面の〔セキュリティー（共通）〕項目にて WPA2 を〔有効〕、固定 WEP、動的 WEP、TKIP をそれぞれ〔無効〕に設定してください。

図4.7-36　Passpoint 設定

Passpoint 機能が〔有効〕の場合、本装置から送信される Beacon フレームと Probe Response フレームに下記エレメントを付与します。各エレメントにフレキシブルな設定が可能です。ここでは各設定画面を紹介します。〔Passpoint 編集〕画面にて設定変更可能です。

表4.7-1　Beacon/Probe Response の付与エレメント一覧表

付与エレメント	各種設定
Interworking	＜設定変更可能＞ ・ネットワークタイプ設定 ・インターネット接続可否設定 ・HESSID 設定 ・Venue Group 設定 ・Venue Type 設定
Roaming Consortium	＜設定変更可能＞ ・ローミングコンソーシアム設定
BSS Load	＜設定変更不可＞ 端末接続台数やチャネル利用率などの状態値を付与します。
Advertisement Protocol	＜設定変更不可＞ 固定値を付与します。
P2P	＜設定変更不可＞ 固定値を付与します。
Hotspot 2.0 Indication	＜設定変更可能＞ ・DGAF 設定

◆ Interworking エレメントに関する設定画面

［Passpoint 編集］画面（図 4.4-35）の［アクセスネットワークタイプ設定］をクリックします。

図4.7-37　アクセスネットワークタイプ設定

［Passpoint 編集］画面（図 4.4-35）の［インターネット接続可否設定］をクリックします。

図4.7-38　インターネット接続可否設定

［Passpoint 編集］画面（図 4.4-35）の［HESSID 設定］をクリックします。

図4.7-39　HESSID 設定

［Passpoint 編集］画面（図 4.4-35）の［Venue Info 設定］をクリックします。

図4.7-40　　Venue Info 設定

［Venue Info 設定］画面（図 4.4-40）の［一覧参照］をクリックします。

Venueタイプ一覧

Venueグループ		Venueタイプ	
番号 *1	詳細	番号 *1	詳細
0	未指定	0	未指定
1	集合場所	0	未指定
		1	アリーナ
		2	スタジアム
		3	ターミナル
		4	円形劇場
		5	遊園地
		6	礼拝所
		7	会議場
		8	図書館
		9	博物館
		10	レストラン
		11	映画館
		12	バー
		13	コーヒーショップ
		14	動物園または水族館
		15	緊急対応センター
2	ビジネス	0	未指定
		1	診療所または歯科医院
		2	銀行
		3	消防署
		4	警察署
		5	（予約）
		6	郵便局
		7	専門家事務所
		8	研究開発施設
		9	弁護士事務所
3	教育	0	未指定
		1	小学校
		2	中等学校
		3	大学
4	工業	0	未指定
		1	工場
5	施設	0	未指定
		1	病院
		2	介護施設
		3	アルコール＆薬物リハビリセンター
		4	グループホーム
		5	刑務所または留置所
6	商業	0	未指定
		1	小売店
		2	マーケット
		3	自動車サービスステーション
		4	ショッピングモール
		5	ガソリンスタンド
7	住居	0	未指定
		1	個人住居
		2	ホテルまたはモーテル
		3	寮
		4	下宿
8	倉庫	0	未指定
9	多目的	0	未指定
10	乗り物	0	未指定
		1	自動車またはトラック
		2	飛行機
		3	バス
		4	フェリー
		5	船またはボート
		6	列車
		7	バイク
11	屋外	0	未指定
		1	市営メッシュネットワーク
		2	都市公園
		3	休憩所
		4	交通管制
		5	バス停留所
		6	キオスク

*1　グループ、タイプのそれぞれの空いている番号(～255)は予約番号となります。

閉じる

図4.7-41　　Venue タイプ一覧

◆ Roaming Consortium エレメントに関する設定画面

［Passpoint 編集］画面（図 4.4-35）の［ローミングコンソーシアム設定］をクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

ローミングコンソーシアム設定

設定番号	1
設定タイプ	◉ OUI ○ OUI-36
Organization Identifier *5	(HEX:区切りなしの場合6桁または10桁、区切りありの場合8桁または14桁)

図4.7-42　ローミングコンソーシアム設定

Passpoint 機能の 1 つである「ネットワークの発見および選択」にあたり、本装置では端末からの GAS プロトコルを用いた問い合わせに対応しています。本装置から送信される GAS Initial Response フレームに下記エレメントを付与します。各エレメントにフレキシブルな設定が可能です。ここでは各設定画面を紹介します。〔Passpoint 編集〕画面にて設定変更可能です。

表4.7-2　GAS Initial Response の付与エレメント一覧表

付与エレメント	各種設定
ANQP	＜設定変更可能＞ ・Venue Name 設定 ・ネットワーク認証種別設定 ・HTTP/HTTPS リダイレクション URL 設定 ・IPv4 アドレス利用可否設定 ・IPv6 アドレス利用可否設定 ・NAI Realm 設定 ・EAP メソッド設定 ・MCC 設定 ・MNC 設定 ・ドメイン名設定
Hotspot 2.0 ANQP	＜設定変更可能＞ ・オペレータフレンドリー名設定 ・リンク速度設定 ・コネクション状態設定

◆ ANQP エレメントに関する設定画面

［Passpoint 編集］画面（図 4.4-35）の［Venue Name 設定］をクリックします。

図4.7-43　Venue Name 設定

［Passpoint 編集］画面（図 4.4-35）の［ネットワーク認証種別設定］をクリックします。

図4.7-44　ネットワーク認証種別設定

［Passpoint 編集］画面（図 4.4-35）の［HTTP/HTTPS リダイレクション URL 設定］をクリックします。

図4.7-45　HTTP/HTTPS リダイレクション URL 設定

［Passpoint 編集］画面（図 4.4-35）の［IPv4 アドレス利用可否設定］をクリックします。

図4.7-46　IPv4 アドレス利用可否設定

［Passpoint 編集］画面（図 4.4-35）の［IPv6 アドレス利用可否設定］をクリックします。

図4.7-47　IPv6 アドレス利用可否設定

［Passpoint 編集］画面（図 4.4-35）の［NAI Realm 設定］をクリックします。

図4.7-48　NAI Realm 設定

［Passpoint 編集］画面（図 4.4-35）の［EAP メソッド設定］をクリックします。

図4.7-49　EAP メソッド設定

［Passpoint 編集］画面（図 4.4-35）の［MCC 設定］をクリックします。

図4.7-50　MCC 設定

［Passpoint 編集］画面（図 4.4-35）の［MNC 設定］をクリックします。

図4.7-51　MNC 設定

［Passpoint 編集］画面（図 4.4-35）の［ドメイン名設定］をクリックします。

図4.7-52　ドメイン名設定

◆ Hotspot 2.0 ANQP エレメントに関する設定画面

［Passpoint 編集］画面（図 4.4-35）の［オペレータフレンドリー名設定］をクリックします。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

オペレータフレンドリー名設定

日本語 *3	Wi-Fi Alliance (0~63文字)
英語 *3	Wi-Fi Alliance (0~63文字)
中国語 *3	Wi-Fi联盟 (0~63文字)

図4.7-53　　オペレータフレンドリー名設定

［Passpoint 編集］画面（図 4.4-35）の［リンク速度設定］をクリックします。

図4.7-54　　リンク速度設定

［Passpoint 編集］画面（図 4.4-35）の［コネクション状態設定］をクリックします。

図4.7-55　　コネクション状態設定

また、本装置から端末へのグループアドレス宛フレームの転送（Downstream Group-Address Forwarding）有無を切り替えることが可能です。

設定手順

手順1　〔SSID 管理〕 → 〔Passpoint 設定〕を選択します。

図4.7-56　メニュー（Passpoint 設定）

手順2　対象となる SSID の〔編集〕ボタンをクリックします。

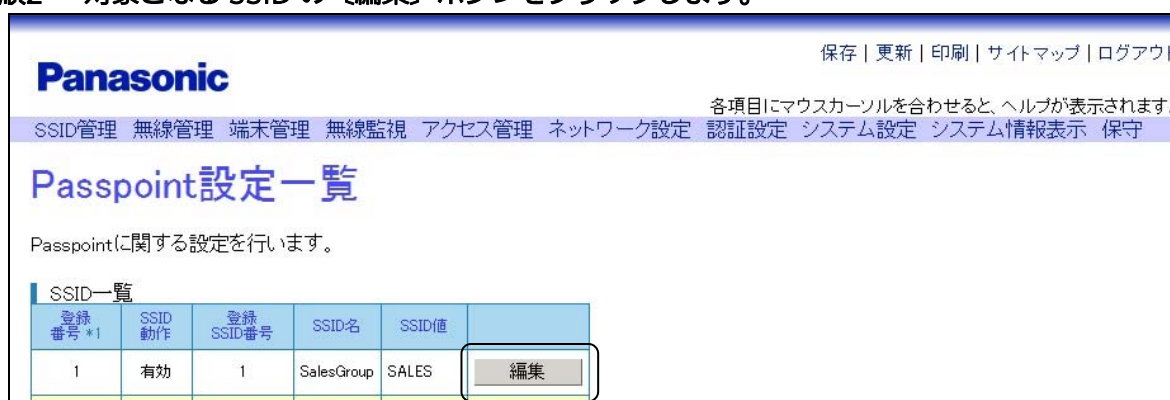



図4.7-57　Passpoint 設定一覧（SSID 一覧）

手順3　〔DGAF 設定〕をクリックします。

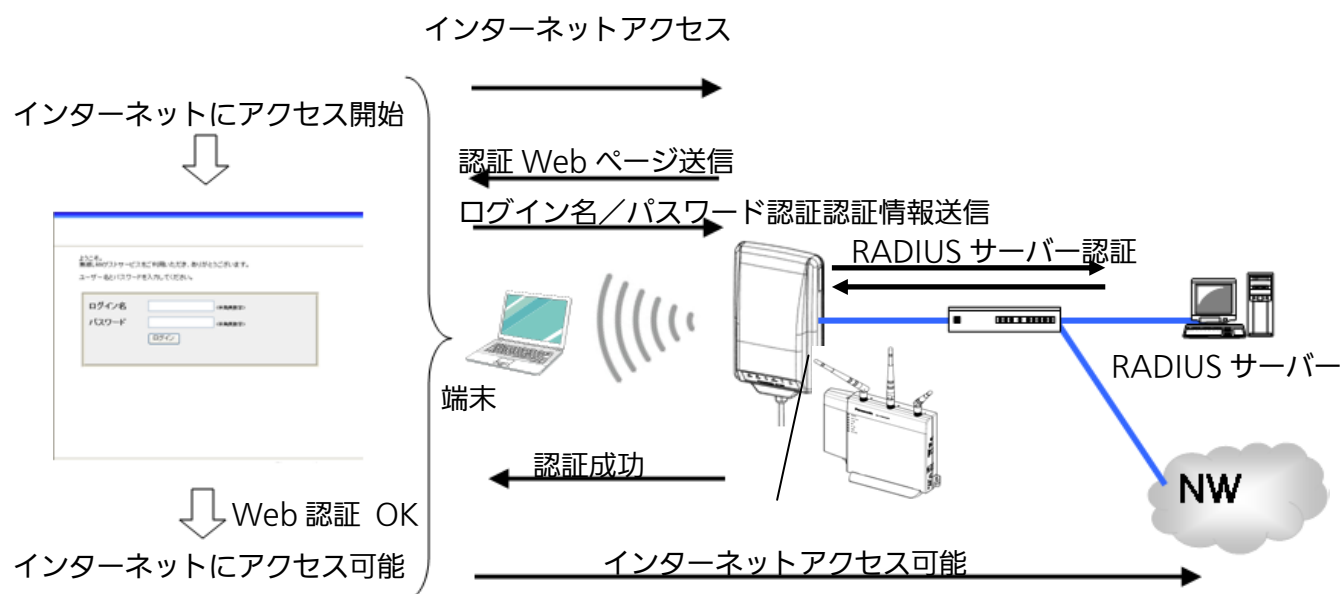
図4.7-58　Passpoint 編集

手順4　DGAF 設定を〔有効〕または〔無効〕にします。

DGAF 設定の初期値は〔有効〕です。DGAF 設定を〔無効〕にすると、〔SSID 編集〕画面の〔代理 ARP 応答動作〕の設定に関わらず、代理 ARP 応答動作が〔未学習端末宛てフレーム破棄〕となります。

図4.7-59　DGAF 設定

4.8　Web認証

Web 認証では、ユーザーが特別なソフトウェアを導入することなく、一般的に使用されている Web ブラウザのみを使用することで認証処理を行うことができます。ネットワーク利用の際には、Web ブラウザ上でログイン名とパスワードでの認証を行い､成功したユーザーのみがネットワークにアクセスできるようになります。
端末のブラウザに表示される認証画面の例を紹介します。

ここでは、Web 認証の各種設定方法を紹介します。

4.8.1　Web認証一覧

設定手順

◆ Proxy 設定（Web 認証）

外部のネットワークにアクセスする際に、Web Proxy サーバーを使用する環境においても、Web 認証が実施できるよう、Web Proxy サーバーを登録します。SSID ごとに 16 個まで設定できます。

手順1　〔認証設定〕　→　〔Web 認証〕　→　〔Web 認証設定一覧〕を選択します。

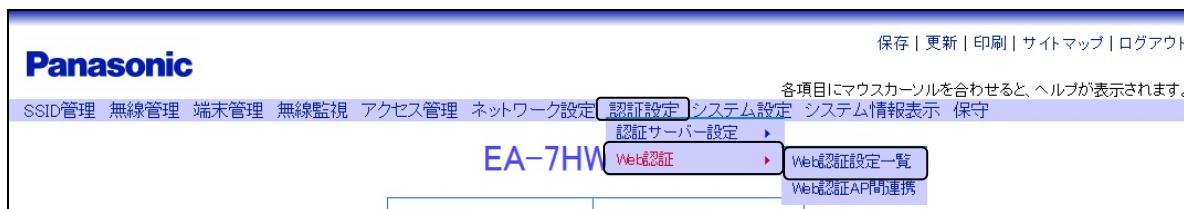



図4.8-1　　メニュー（Web 認証設定一覧）

手順2　対象となる SSID の“Proxy 設定”を選択し、〔編集〕ボタンをクリックします。
※例として、登録番号 1 番に対して設定を行います。

図4.8-2　Web 認証設定一覧

手順3　〔Proxy サーバー設定〕ボタンをクリックします。

図4.8-3　Proxy 設定（Web 認証）

手順4　対象となる Proxy サーバーの設定を行います。
例として、下記内容での設定を示します。

・ 登録番号〔1〕を選択
・ IP アドレスに　「1.72.197.139」を入力
・ TCP ポート番号に「8080」を入力

画面最下部の〔設定〕ボタンを押し、設定を反映させせます。

図4.8-4　Proxy サーバー設定

手順5　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。
設定反映が正常に行われると、下記画面のように表示されます。

図4.8-5　Proxy サーバー一覧

設定手順

◆ 認証除外設定

指定した IP アドレスとの IP パケットの送受信に対しては、Web 認証状態が未認証であっても、端末と該当ホスト間の IP パケットを透過させることが可能です。認証除外設定対象のホストは、個々の SSID ごとに対し、最大 32 アドレスまで指定が可能です。対象ホストの情報は IP アドレスとサブネットマスク値の組み合わせで保持され、ネットワーク部が一致するホストとの送受信を透過させます。

手順1　〔認証設定〕　→　〔Web 認証〕　→　〔Web 認証設定一覧〕を選択します。

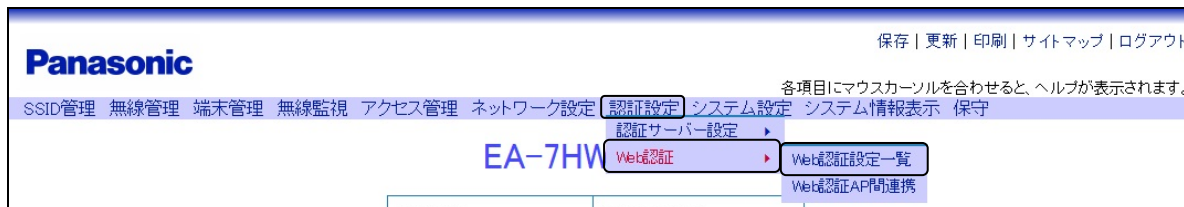



図4.8-6　メニュー（Web 認証設定一覧）

手順2　対象となる SSID の “認証除外設定” を選択し、〔編集〕ボタンをクリックします。
※　例として、登録番号 2 番に対して設定を行います。

図4.8-7　Web 認証設定一覧表（認証除外設定）

手順3　〔認証除外アドレス設定〕ボタンをクリックします。

図4.8-8　認証除外設定（認証除外アドレス設定）

手順4　対象となる認証除外アドレスの設定を行います。

例として、下記内容での設定を示します。

- 登録番号〔2〕を選択
- IP アドレスに　「1.72.197.139」を入力
- マスク値に「255.255.255.0」を入力
  （フルアドレスマスクにより　ホストの指定も可能（マスクは中抜き可能））

画面最下部の〔設定〕ボタンを押し、設定を反映させます。

図4.8-9　認証除外アドレス設定

手順5　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

設定反映が正常に行われると、下記画面のように表示されます。

図4.8-10　認証除外一覧

設定手順

◆ Web 認証ログイン画面設定

通信事業者様ごとに個別のログインページのデザイン（ロゴなど）にできるよう、SSID ごとにログインページを設定することができます。

手順1　〔認証設定〕　→　〔Web 認証〕　→　〔Web 認証設定一覧〕を選択します。対象となる SSID の “Web 認証ログイン画面設定” を選択し、〔編集〕ボタンをクリックします。

例として、登録番号 3 番に対して設定を行います。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守
認証サーバー設定
Web認証
Web認証設定一覧
Web認証AP間連携
EA-7HW

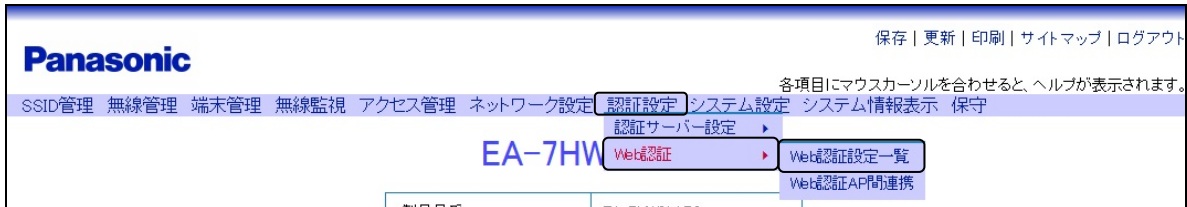



図4.8-11　メニュー（Web 認証設定一覧）

手順2　対象となる SSID の “Web 認証ログイン画面設定” を選択し、〔編集〕ボタンをクリックします。

例として、登録番号 3 番に対して設定を行います。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

Web認証設定一覧

Web認証に関する設定を行います。

SSID一覧

登録番号 *1	SSID動作	登録SSID番号	SSID名	SSID値		
1	有効	1	SalesGroup	SALES	Proxy設定	編集
2	有効	2	PlanningGroup	Planning	Proxy設定	編集
3	有効	3	DevelopmentGroup	Development	Proxy設定	編集
4	無効				Proxy設定 認証除外設定 Web認証ログイン画面設定	編集

図4.8-12　Web 認証設定一覧表（Web 認証ログイン画面設定）

手順3　〔Web 認証ログイン画面設定〕ボタンをクリックします。

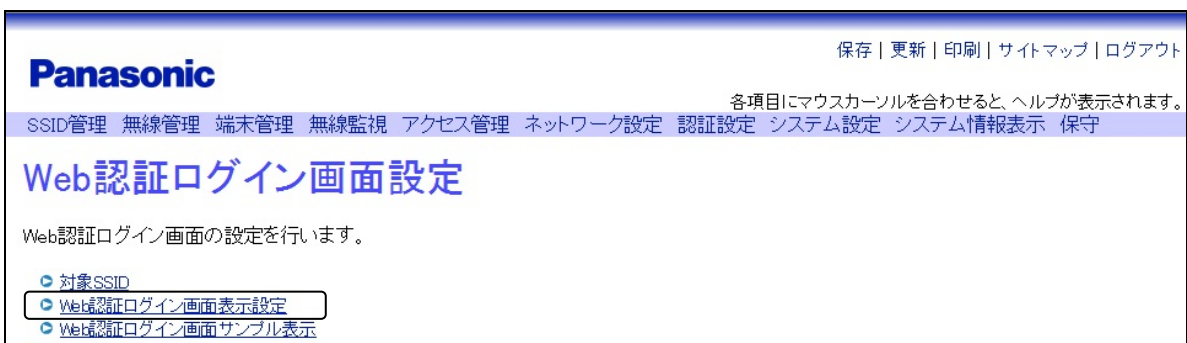



図4.8-13　Web 認証ログイン画面設定

手順4　対象となる Web 認証ログイン画面の設定を行います。

例として、下記内容での設定を示します。

- タイトルテキスト設定「Capital Portal Login」を入力
- 組織名設定に　「Panasonic Corporation」を入力
- ログインメッセージ設定に「ようこそ。
無線 LAN ゲストサービスをご利用いただき、ありがとうございます。

ユーザー名とパスワードを入力してください。」を入力
- フッタテキスト設定「ご利用方法は無線 LAN アクセス管理サイトへ」を入力
- メインロゴ URI 設定に　「http://127.0.0.1/main_logo.png」を入力
  ※メインロゴを使用しない場合は、メインロゴ URI 設定の入力欄を空欄にしてください。メインロゴを使用する場合、メインロゴ URI のホスト部に記載された IP アドレスは、認証除外設定が必要です。

- 利用条件メッセージ表示設定の〔有効〕を選択
- 利用条件メッセージ設定に　「本サービスのご利用にあたっては弊社が定める規約に
準拠していただく必要があります。

よろしければ、承認をチェックしてください。」を入力

図4.8-14　Web 認証ログイン画面表示設定

手順5　上記設定終了後、画面最下部の〔設定〕ボタンを押し、設定を反映させます。

設定反映が正常に行われると、下部画面のように表示されます。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

Web認証ログイン画面表示設定

項目	設定値	文字数
タイトルテキスト設定 *1	Captive Portal Login	(0~32文字)
組織名設定 *1	Panasonic Corporation	(0~64文字)
ログインメッセージ設定 *1	ようこそ。 無線LANゲストサービスをご利用いただき、ありがとうございます。 ユーザー名とパスワードを入力し	(0~128文字)
フッタテキスト設定 *1	ご利用方法は無線LANアクセス管理サイトへ	(0~256文字)
メインロゴURI設定	http://127.0.0.1/main_logo.png	(0~128文字)
利用条件メッセージ表示設定	有効　無効	
利用条件メッセージ設定 *1	本サービスのご利用にあたっては弊社が定める規約に 準拠していただく必要があります。 よろしければ、承認	(0~512文字)

図4.8-15　Web 認証ログイン画面表示

手順6　〔Web 認証ログイン画面サンプル表示〕ボタンをクリックします。

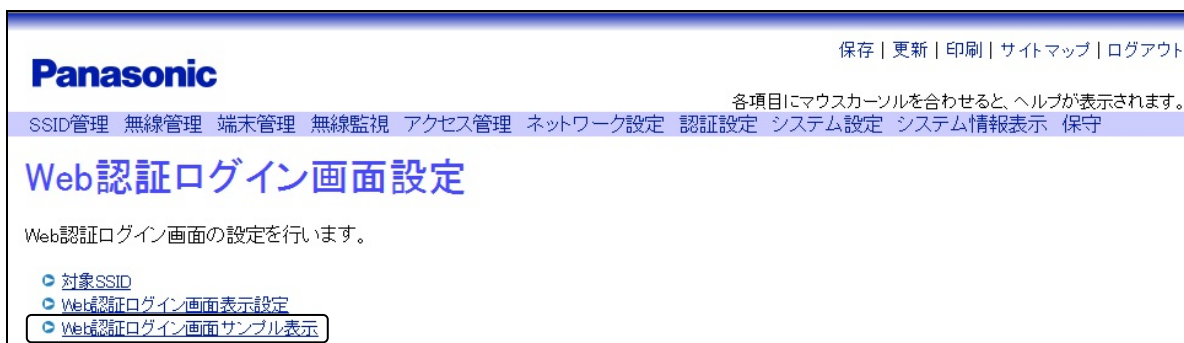



図4.8-16　Web 認証ログイン画面サンプル表示

手順7　サンプル画面表示の〔表示〕ボタンをクリックします。

図4.8-17　サンプル画面表示

手順8　手順 4 で設定したサンプル画面を確認することが出来ます。

図4.8-18　サンプル画面

設定手順

◆ リダイレクト先 URL 設定

Web 認証成功時に端末にリダイレクトさせるアクセス先 URL を設定することが出来ます。本設定は SSID 毎に 1 つずつ設定することが可能です。

手順1 〔認証設定〕 → 〔Web 認証〕 → 〔Web 認証設定一覧〕を選択します。

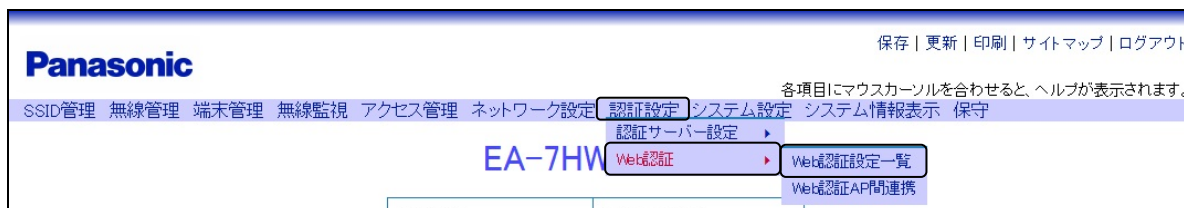



図4.8-19 メニュー（Web 認証設定一覧）

手順2 対象となる SSID の“アクセス先 URL 設定”を選択し、〔編集〕ボタンをクリックします。

例として、登録番号 3 番に対して設定を行います。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守

Web認証設定一覧

Web認証に関する設定を行います。

SSID一覧

登録番号 *1	SSID動作	登録SSID番号	SSID名	SSID値		
1	有効	1	wwwwwwwwwwwwwwwww	wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww	Proxy設定	編集
2	無効				Proxy設定	編集
3	有効	15	SSID015	HotSpot015	アクセス先URL設定	編集
4	有効	16	SSID016	HotSpot016	Proxy設定 認証除外設定 Web認証ログイン画面設定 アクセス先URL設定	編集
5	有効	13	SSID013	HotSpot013	Proxy設定	編集

図4.8-20 Web 認証設定一覧表（アクセス先 URL 設定）

手順3 アクセス先 URL の設定を行います。

例として、[http://panasonic.jp/]をアクセス先 URL として設定を行います。
入力する URL は「http://」もしくは、「https://」から入力してください。
指定可能な最大 URL 長は 255 文字です。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

Web認証完了後にアクセスするURLの設定を行います。

- 対象SSID
- アクセス先URL設定

対象SSID

SSID番号	16
SSID名	SSID16

このページのTopへ

アクセス先URL設定

アクセス先URL *1	http://panasonic.jp/	(0～255文字)

*1 「http://」、もしくは、「https://」から入力してください。

このページのTopへ

設定

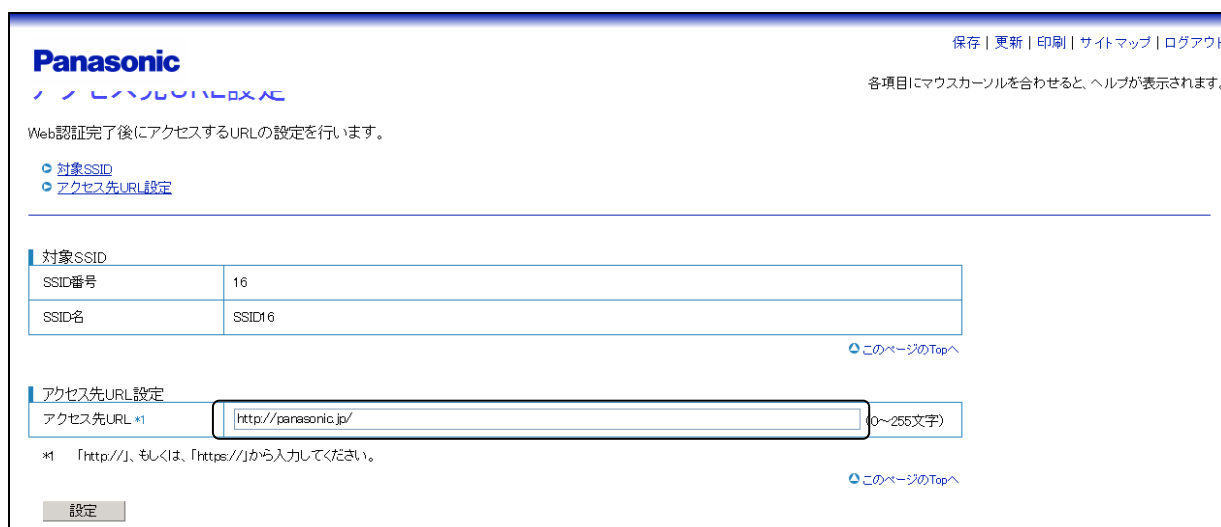



図4.8-21 アクセス先 URL 設定

手順4　上記設定終了後、画面最下部の[設定]ボタンを押し、設定を反映させます。

設定反映が正常に行われると、下部画面のように表示されます。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

アクセス先URL設定

Web認証完了後にアクセスするURLを設定することができます。

- 対象SSID
- アクセス先URL設定

対象SSID

SSID番号	16
SSID名	SSID16

このページのTopへ

アクセス先URL設定

アクセス先URL *1	http://panasonic.jp/ (0～255文字)

*1　「http://」、もしくは、「https://」から入力してください。

このページのTopへ

図4.8-22　アクセス先 URL 設定画面

4.8.2　Web認証AP間連携

　端末が移動によりハンドオーバーして、接続先 AP が変更した場合、接続先 AP における Web 認証を省略することが可能です。そのため、初回接続先の AP において、端末の Web 認証が完了した際に、周辺 AP に対して当該端末が認証済みであることを通知することにより Web 認証情報を共有します。
　AP は、端末接続時に Web 認証共有情報を参照し、接続端末の MAC アドレスが登録されている場合は、Web 認証済みとして扱い、改めて Web 認証処理を行うことなく、外部との通信を可能とさせます。

設定手順

端末が初回接続で Web 認証を行った際に、その Web 認証情報を通知する AP を設定します。通知先 AP は 2 ヶ所まで設定できます。

手順1　〔認証設定〕　→　〔Web 認証〕　→　〔Web 認証 AP 間連携〕を選択します。

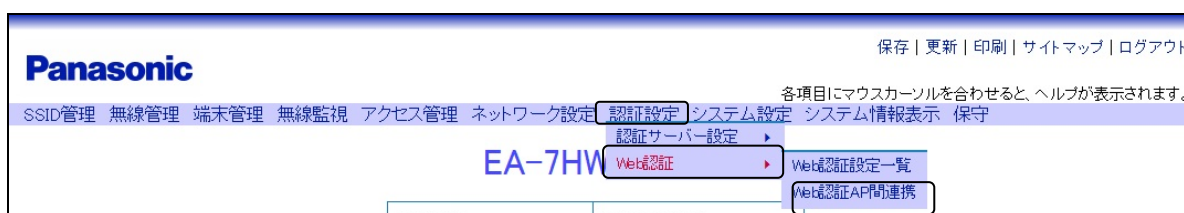



図4.8-23　　メニュー（Web 認証 AP 間連携）

手順2　〔Web 認証生存時間〕をクリックします。

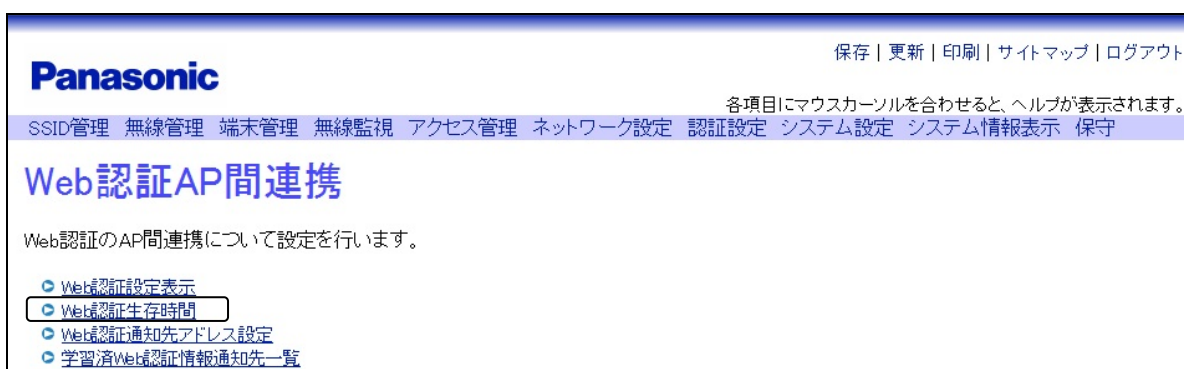



図4.8-24　　Web 認証 AP 間連携

手順3　〔Web 認証生存時間〕の設定します。

〔Web 認証生存時間〕を設定します。

例として、下記内容での設定を示します。

・　タイマー初期値に「1440」を入力

〔設定〕ボタンを押し、設定を反映させせます。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

Web認証生存時間

タイマー初期値	1440 分 (10~1440)

図4.8-25　Web 認証生存時間

手順4　〔Web 認証通知アドレス〕の設定します。

〔Web 認証通知アドレス〕の設定を行います。

例として、下記内容での設定を示します。

・　通知先番号〔1〕を選択

・　IP インターフェース番号〔2〕を選択

・　通知先 IP アドレスに「192.168.0.200」を入力

〔設定〕ボタンを押し、設定を反映させせます。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

このページのTopへ

Web認証通知先アドレス設定

通知先番号	1
IPインターフェース番号	2
通知先IPアドレス	192.168.0.200 (xxx.xxx.xxx.xxx [xxx=0~255])

図4.8-26　Web 認証通知先アドレス設定

手順5　上記設定終了後、設定が反映させたことを確認します。

設定反映が正常に行われると、下記画面のように表示されます。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

Web認証設定表示

Web認証生存時間		1440 分
通知先番号1	通知先IPアドレス	192.168.0.200
	IPインターフェース番号	2
通知先番号2	通知先IPアドレス	192.168.0.100
	IPインターフェース番号	2

図4.8-27　Web 認証設定表示

4.9　その他の機能

その他の機能として、SSID ごとに設定を行う「アグリゲーション」、「LDPC 符号化」について説明します。

設定手順

手順1　〔SSID 管理〕　→　〔SSID 設定〕を選択します。

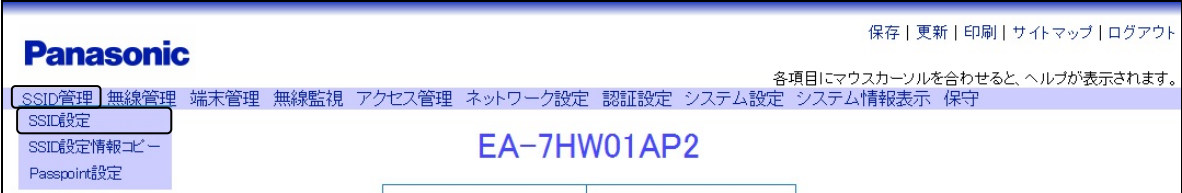



図4.9-1　メニュー（SSID 設定）

手順2　〔SSID 一覧〕をクリックします。

図4.9-2　SSID 設定

手順3　対象となる SSID の〔編集〕ボタンをクリックします。

SSID番号	SSID名	SSID値（先頭の20文字を表示します）	VLANモード	SSID VLAN-ID	スイッチングモード設定	
1	SalesGroup		OFF	1	折り返しあり	編集

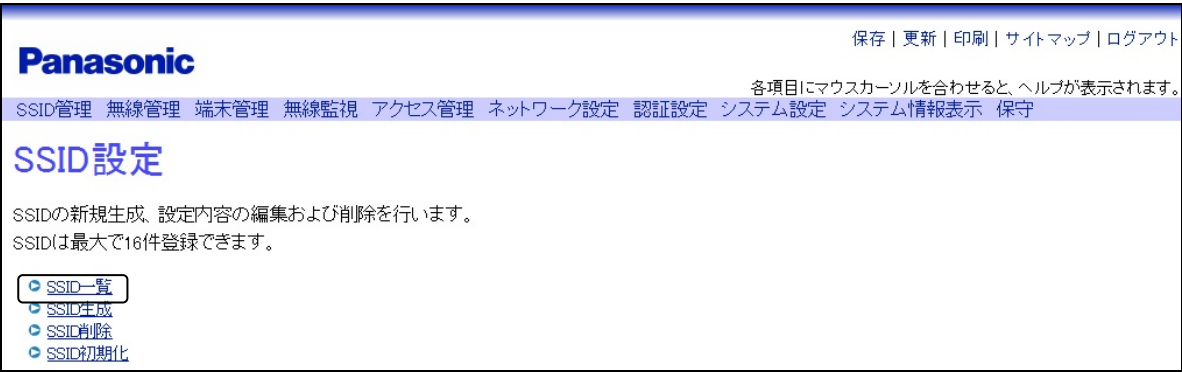



図4.9-3　SSID 一覧

〔SSID 編集〕画面（図 4.9-4）が表示されます。前述の機能設定はこちらより行います。

図4.9-4　SSID 編集

■アグリゲーション

高速化通信を実現するため、フレームを連結する方式として、A-MPDU と A-MSDU の 2 種類が存在しています。

アグリゲーションでは、「OFF」「A-MPDU」「A-MSDU」「A-MPDU＋A-MSDU」（4 パターン）のいずれかを選択します。

〔SSID 編集〕画面（図 4.9-4）の〔アグリゲーション〕をクリックします。

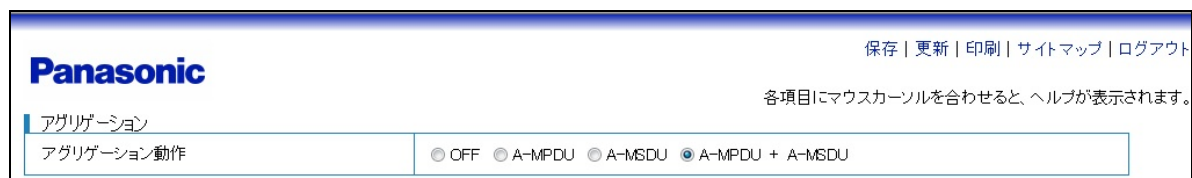



図4.9-5　アグリゲーション

■LDPC 符号化

アソシエーション時に、本装置で〔LDPC 符号化〕が有効、かつ端末が LDPC 対応である場合に限り、LDPC 符号を使用します。〔無効〕を選択した場合は「畳み込み符号を使用」となります。

〔SSID 編集〕画面（図 4.9-4）の〔LDPC 符号化〕をクリックします。

図4.9-6　LDPC 符号化

第５章　VPNネットワーク対応

VPN ネットワーク構築の設定手順について、説明します。

5.1　L2TP over PPPoE ネットワーク接続での設定

ここでは、PPPoE でインターネットに接続している 2 つの拠点を L2TP で結ぶ VPN 構築例を紹介します。

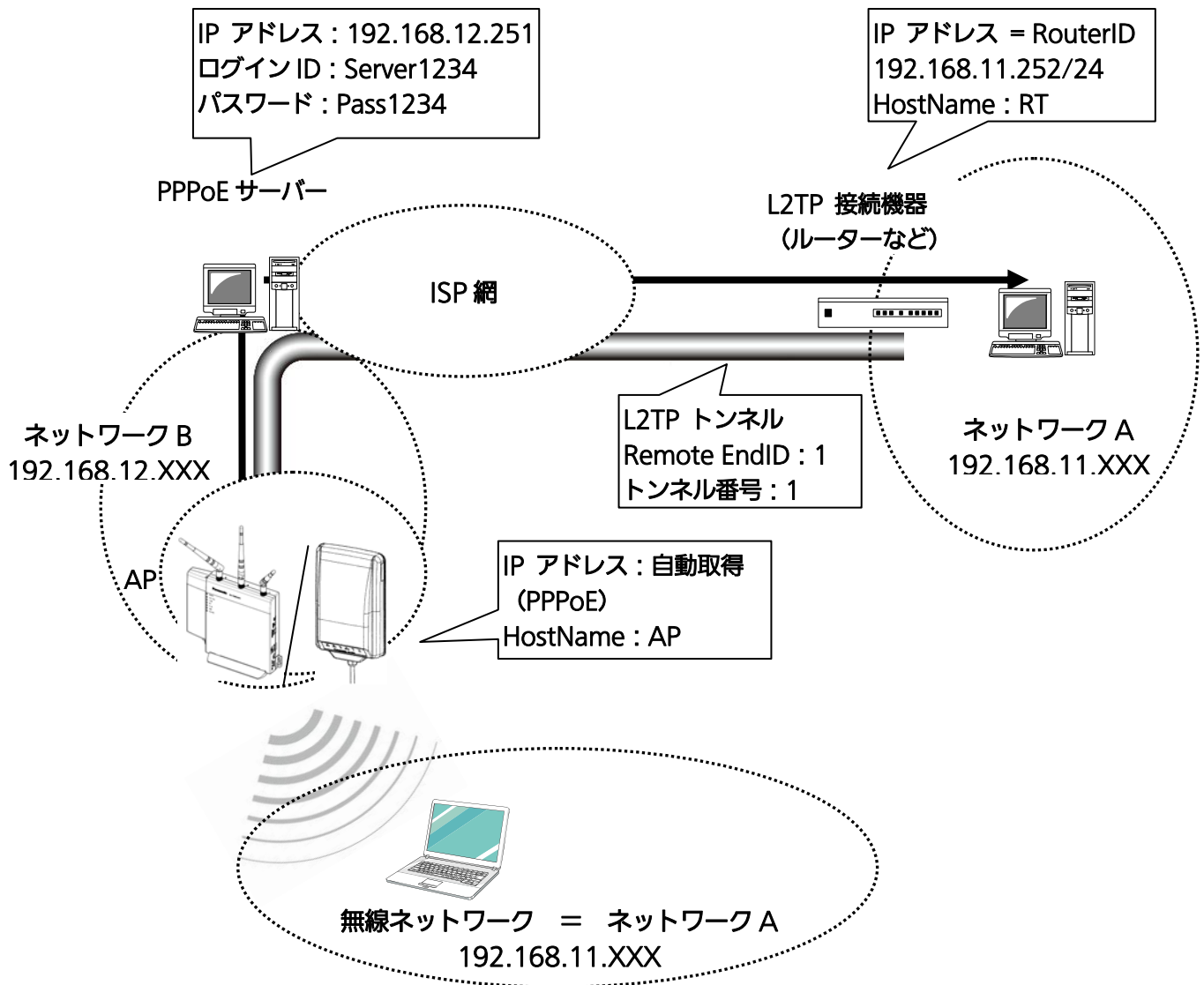



図5.1-1　 ネットワーク構成例（L2TP over PPPoE）

図 5.1-1（L2TP over PPPoE）を構築するための設定は、以下の手順で行います。

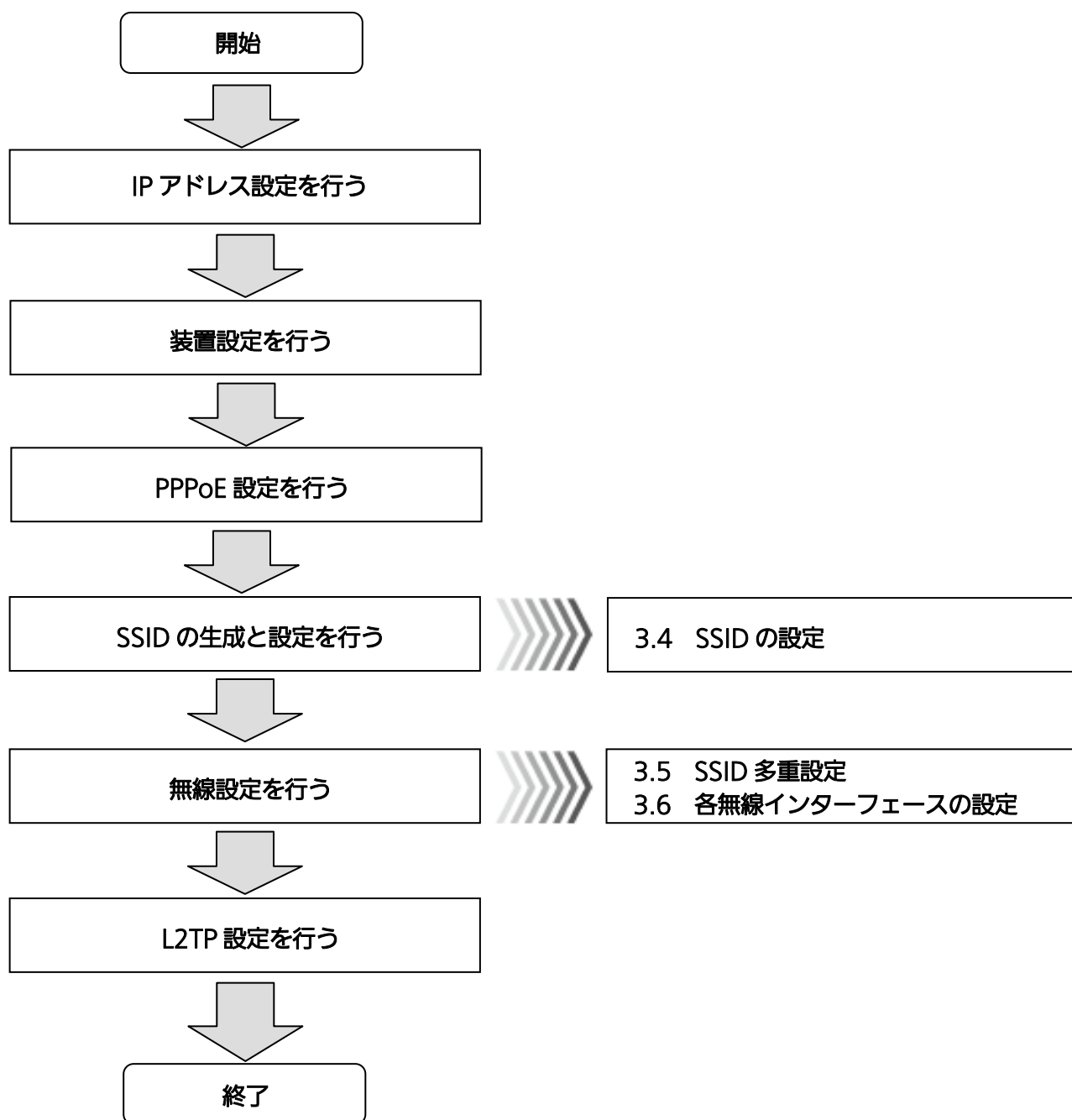



図5.1-2　ネットワーク構成手順（L2TP over PPPoE）

設定手順

◆IP アドレス設定

手順1　〔システム設定〕　→　〔監視インターフェース設定〕
　　　　　　　　　　　　　　　　　→　〔IP アドレス設定〕を選択します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

EA-7HW01AP

運用設定
監視インターフェース設定
監視設定

IPアドレス設定
スタティックルート設定
DHCP再取得設定

製品品番	EA-7HW01AP2

図5.1-3　メニュー（IP アドレス設定）

手順2　対象となる IP インターフェース 1 番の〔編集〕ボタンをクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

IPアドレス設定

自装置のIPアドレスの設定を行います。
完全に独立したIPインターフェースが16個まで登録可能です。IPアドレスなどの設定値は重複登録が可能です。

IPアドレス設定一覧

IP-IF No. *1	状態	動作モード	IPアドレス	サブネットマスク	デフォルトゲートウェイ	VLANモード		
1	有効	Ethernet(自動)	192.168.0.3	255.255.255.0	192.168.0.1	タグなし	編集	再取得
2	有効	Ethernet(固定)	192.168.0.5	255.255.255.0	192.168.0.1	シングルタグ	編集	再取得
3	無効	Ethernet(自動)	---.---.---.---	---.---.---.---	---.---.---.---	タグなし	編集	再取得

図5.1-4　IP アドレス設定

手順 3 ～ 手順 4 は〔IP アドレス編集〕画面（図 5.1-5）より各種設定を行います。

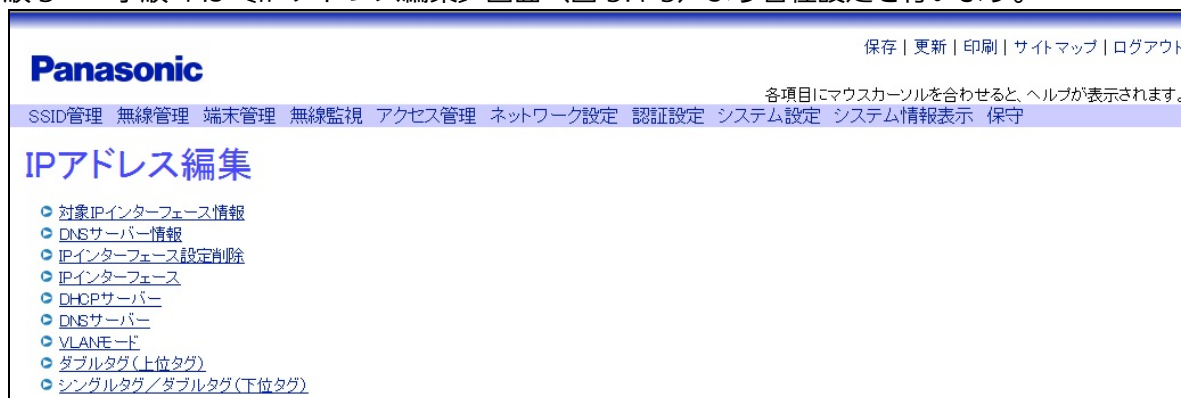



図5.1-5　IP アドレス編集

手順3　〔IP アドレス編集〕画面（図 5.1-5）の IP インターフェースをクリックし、
IP インターフェース 1 番に対して下記設定を行います。

・ インターフェースの〔有効〕を選択
・ 動作モードの〔PPP〕を選択
・ PPP 動作モードの〔Ethernet〕を選択（屋内用無線 LAN アクセスポイントのみ）

※PPP 動作モードの設定変更では、設定した情報を有効にさせるために保存とリセットが必要とな
ります。

図5.1-6　IP インターフェース（屋内用無線 LAN アクセスポイント）

図5.1-7　IP インターフェース（屋外用無線 LAN アクセスポイント）

手順4　画面最下部の〔設定〕ボタンをクリックし、設定を反映させます。

◆装置設定

手順5　〔システム設定〕　→　〔運用設定〕　→　〔装置設定〕を選択します。

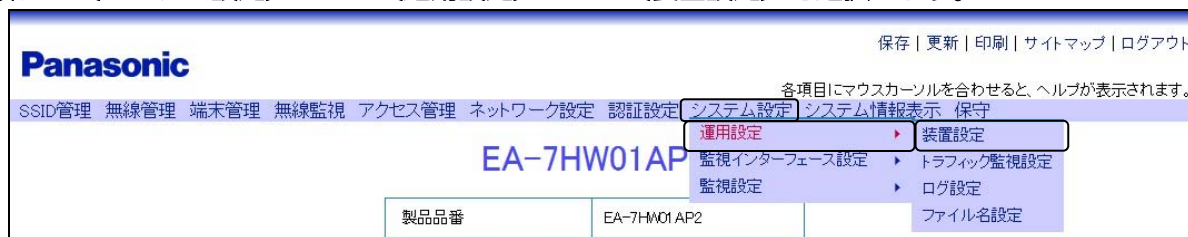



図5.1-8　メニュー（装置設定）

手順6　〔装置情報〕をクリックします。

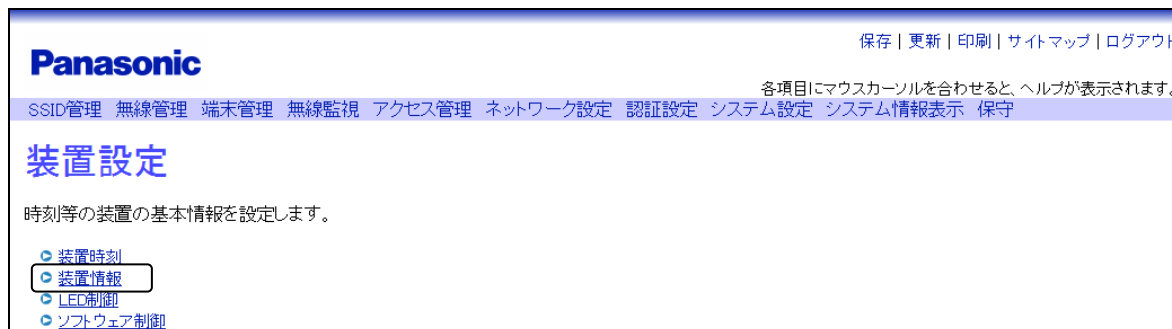



図5.1-9　装置設定（屋内用無線 LAN アクセスポイント）

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守
装置設定
時刻等の装置の基本情報を設定します。
装置時刻
装置情報
ソフトウェア制御

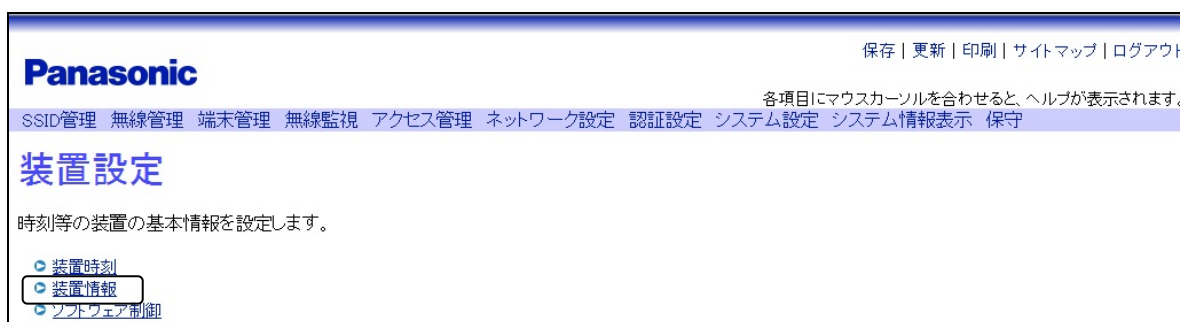



図5.1-10　装置設定（屋外用無線 LAN アクセスポイント）

手順7　装置名称を入力します。
（入力は、半角英数字または半角記号（[?] は除く）　0～255 文字以内で行ってください。）
「装置名称（SysName）」は、L2TP 設定の自装置ホスト名となります。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。

装置情報

装置ロケーション(SysLocation) ※2	
担当者/連絡先(SysContact) ※2	
装置名称(SysName) ※2	AP

※2　入力はすべて半角英数字または半角記号([?]は除く) 0～255文字以内で行ってください。
「装置名称(SysName)」は、L2TP設定の自装置ホスト名となります。
このページのTopへ
設定

図5.1-11　装置情報

手順8　装置情報下部の〔設定〕ボタンを押し、設定を反映させます。

◆PPP 設定

手順9　〔ネットワーク設定〕　→　〔PPP 設定〕を選択します。

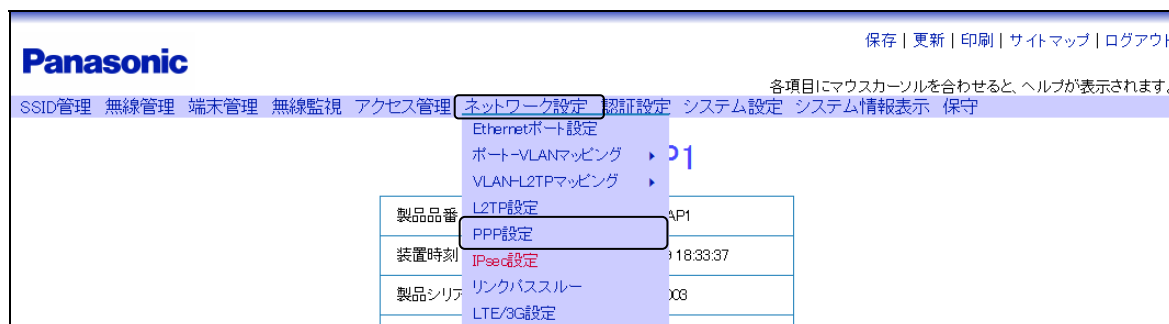



図5.1-12　ネットワーク設定（PPP 設定　屋内用無線 LAN アクセスポイント）

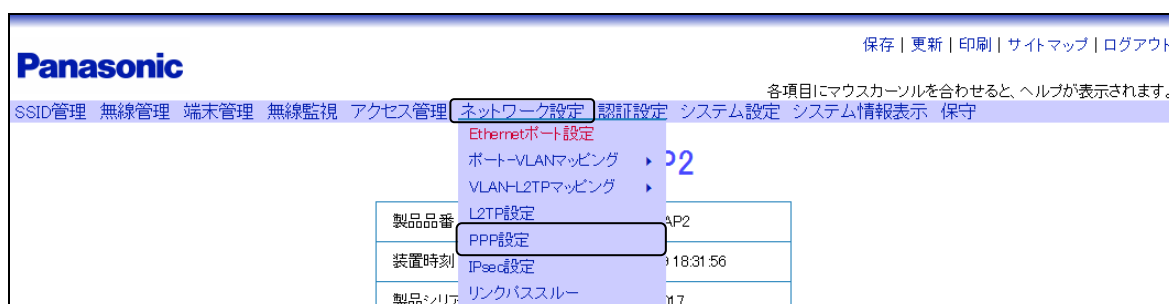



図5.1-13　ネットワーク設定（PPP 設定　屋外用無線 LAN アクセスポイント）

手順 10、手順 11 は〔PPP 設定〕画面（図 5.1-14）より各種設定を行います。

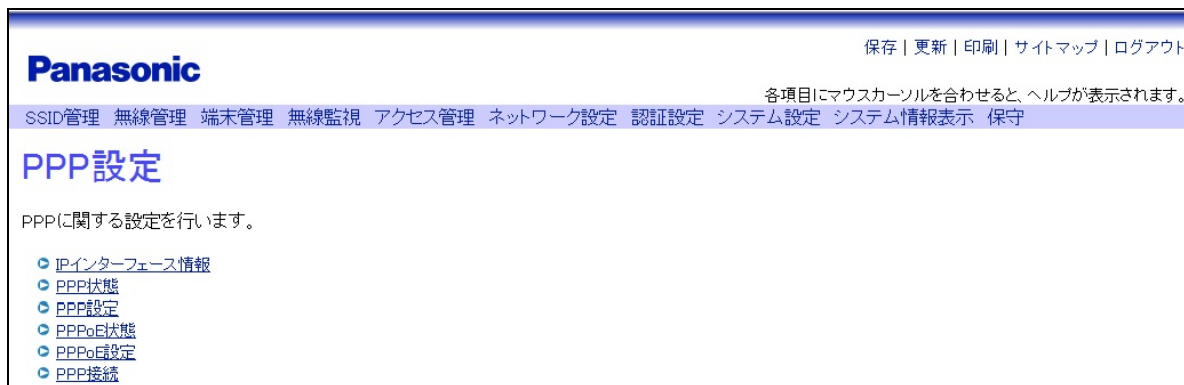



図5.1-14　PPP 設定

手順10　〔PPP 設定〕をクリックし、下記設定を行います。

- 認証方式に〔PAP もしくは CHAP〕を選択
- ログイン名に「Server1234」を入力
- パスワードに「Pass1234」を入力

図5.1-15　　PPP 設定

手順11　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

◆L2TP 設定

手順12　〔ネットワーク設定〕　→　〔L2TP 設定〕を選択します。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

Ethernetポート設定
ポート-VLANマッピング
VLAN-L2TPマッピング
L2TP設定
PPP設定
IPsec設定

製品品番
装置時刻

図5.1-16　　ネットワーク設定（L2TP 設定）

手順 13 ～ 手順 15 は〔L2TP 設定〕画面（図 5.1-17）より各種設定を行います。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

L2TP設定

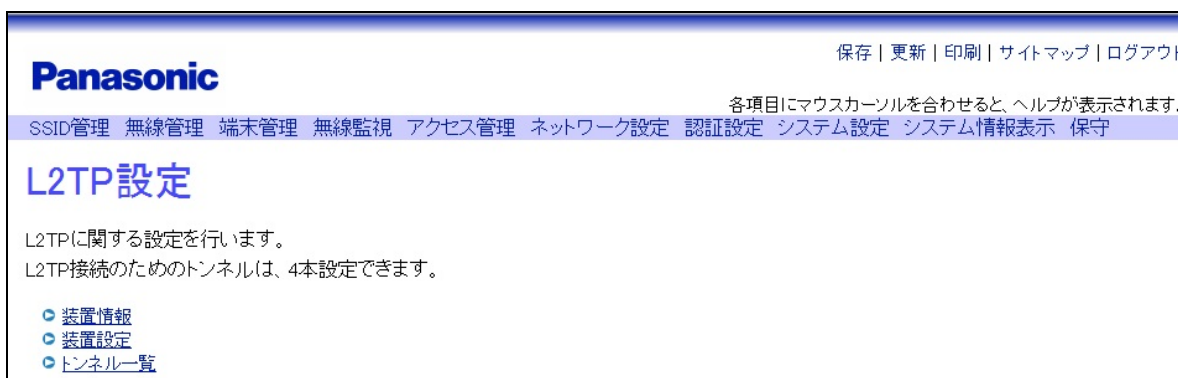
L2TPに関する設定を行います。
L2TP接続のためのトンネルは、4本設定できます。

- 装置情報
- 装置設定
- トンネル一覧

図5.1-17　　L2TP 設定

手順13　〔L2TP 設定〕画面（図 5.1-17）の〔装置情報〕をクリックすることで、〔装置設定〕（図 5.1-11）で入力した自装置ホスト名を確認することができます。

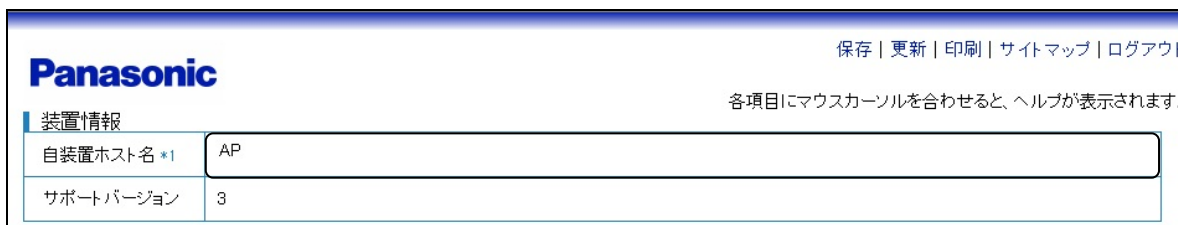



図5.1-18　　装置情報

手順14　〔L2TP 設定〕画面（図 5.1-17）の〔装置設定〕をクリックし、ルーターID に「本装置の IP アドレス」を入力し、〔設定〕ボタンを押して設定を反映させます。

「本装置の IP アドレス」は、PPPoE サーバーとの接続が完了した後、〔IP アドレス設定〕画面（図 5.1-4）で確認してください

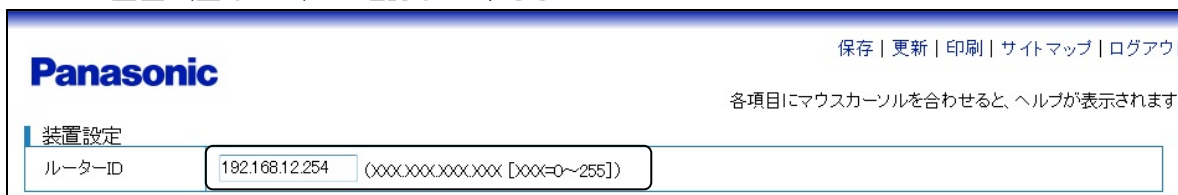



図5.1-19　　装置設定

手順15　〔L2TP 設定〕画面（図 5.1-17）の〔トンネル一覧〕をクリックし、トンネル番号 1 の〔編集〕ボタンをクリックします。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

トンネル一覧

トンネル番号	トンネル機能	カプセル化方式	コネクション状態	接続先IPアドレス	接続先ホスト名（先頭25文字を表示します）	接続先ルーターID	
1	無効	IP	接続中	192.168.255.100	WWWWWWWWWWWWWWWWWWWWWWWWW	192.168.255.100	編集
2	有効	UDP	未接続	192.168.255.100	HOST-2	192.168.255.100	編集
3	有効	IP	コネクション確立	192.168.255.100	HOST-3	192.168.255.100	編集
4	有効	UDP	未設定	192.168.255.100	HOST-4	192.168.255.100	編集

図5.1-20　トンネル一覧

手順 16 ～ 手順 20 は〔L2TP 編集〕画面（図 5.1-21）より各種設定を行います。

図5.1-21　L2TP 編集

手順16　〔L2TP 編集〕画面（図 5.1-21）の対象トンネルをクリックし、トンネル機能の〔有効〕を選択します。

※ カプセル化方式、UDP ポート番号、ベンダーID については、対向装置と設定を合せてください。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

対象トンネル

トンネル番号	1
トンネル機能	◉有効 ○無効
カプセル化方式	◉IP ○UDP
UDPポート番号 *1 *2	1701 (1～9999)
ベンダーID	◉0(標準) ○9(Cisco)

図5.1-22　対象トンネル

手順17　〔L2TP 編集〕画面（図 5.1-21）のコネクションをクリックし、接続開始要求の〔送信〕を選択します。

図5.1-23　コネクション

手順18 〔L2TP 編集〕画面（図 5.1-21）の自装置設定をクリックし、IP インターフェース番号の “ 1 ” を選択します。

図5.1-24　自装置設定

手順19 〔L2TP 編集〕画面（図 5.1-21）の接続先設定をクリックし、下記内容を入力します。

・ 接続先 IP アドレス：192.168.11.252
・ 接続先ホスト名：RT
・ 接続先ルーターID：192.168.11.252
・ 接続用 EndID：1
　※ 接続用 EndID については、対向装置と設定を合せてください。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

接続先設定

コネクションID	25368
接続先IPアドレス *3	192.168.11.252 (xxx.xxx.xxx.xxx [xxx=0～255])
接続先ホスト名 *3 *4	RT (0～255文字)
接続先ルーターID *3	192.168.11.252 (xxx.xxx.xxx.xxx [xxx=0～255])
接続用EndID	1 (0～4294967295)

図5.1-25　接続先設定

手順20 画面最下部の〔設定〕ボタンを押し、設定を反映させます。

5.2　L2TP over IPsec ネットワーク接続での設定

ここでは、L2TP に IPsec を併用することでデータの機密性や完全性を確保した VPN 接続を実現するための基本的な設定方法を説明します。
なお、L2TP 接続先装置の設定については、設置機器の装置マニュアルを別途参照してください。

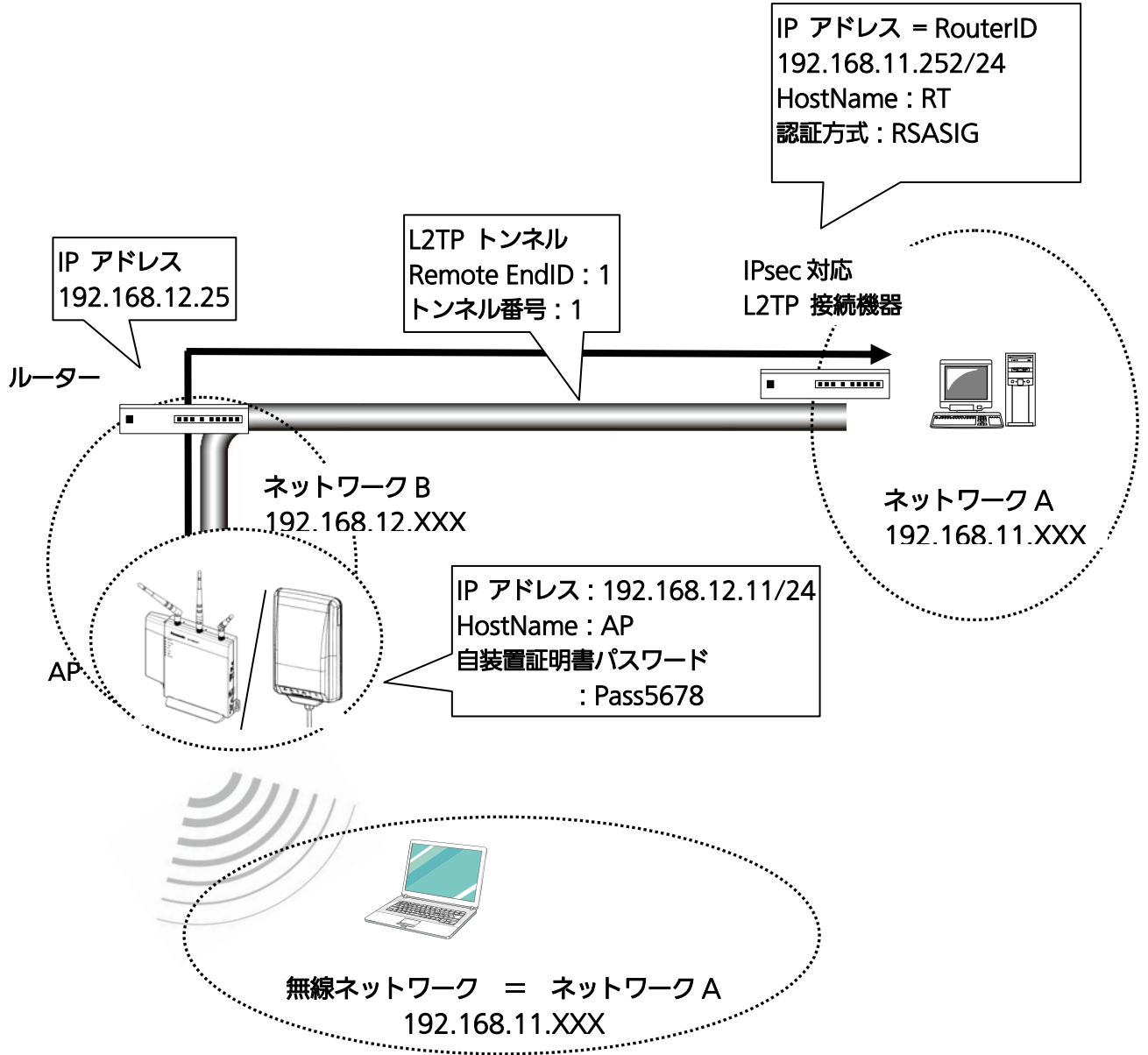



図5.2-1　 ネットワーク構成例（L2TP over IPsec）

図 5.2-1（L2TP over IPsec）を構築するための設定は、以下の手順で行います。

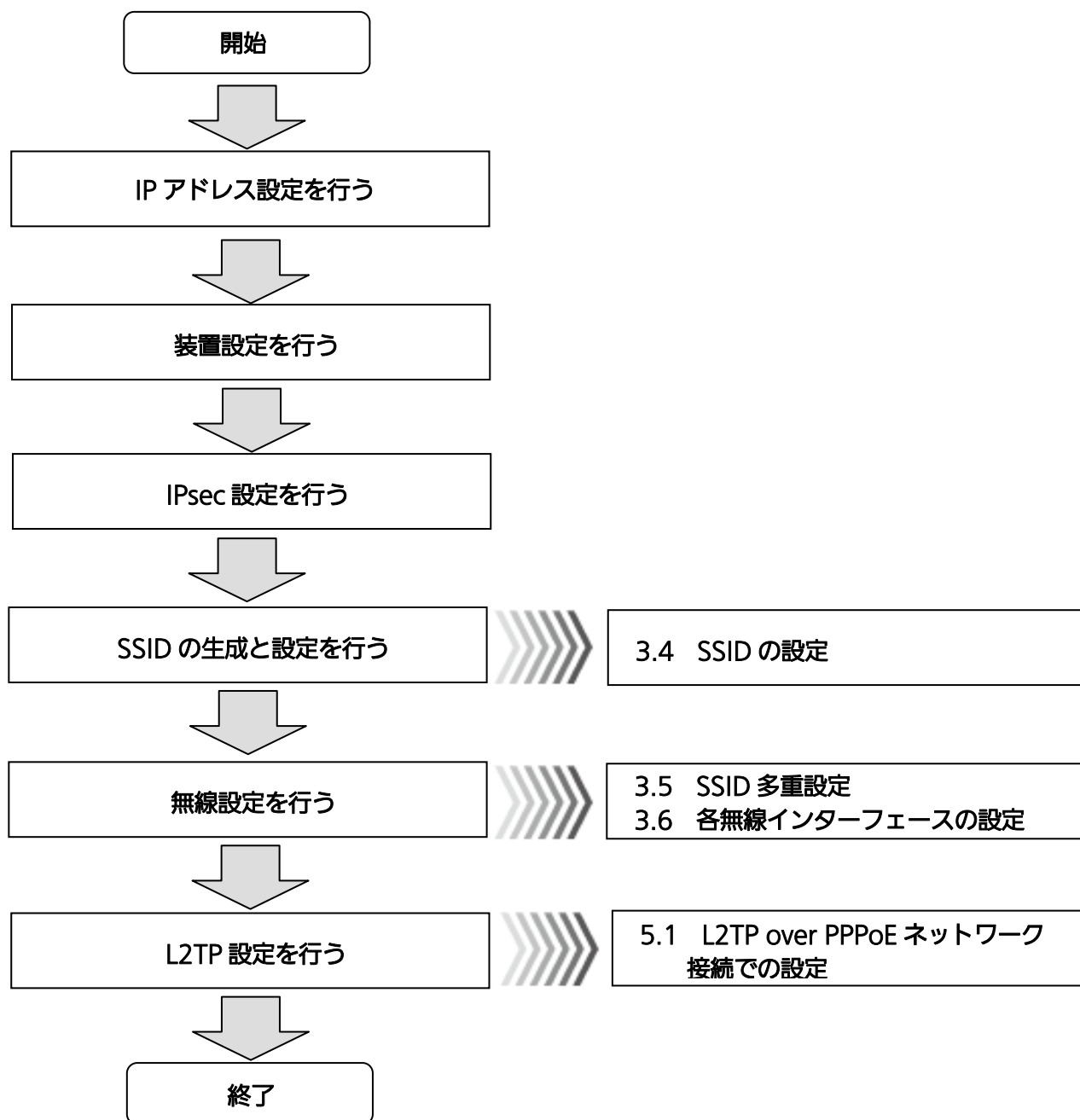



図5.2-2　ネットワーク構成手順（L2TP over IPsec）

設定手順

◆IP アドレス設定

手順1　〔システム設定〕 → 〔監視インターフェース設定〕 → 〔IP アドレス設定〕を　選択します。

図5.2-3　メニュー（IP アドレス設定）

手順2　対象となる IP インターフェース 1 番の〔編集〕ボタンをクリックします。

IP-IF No. *1	状態	動作モード	IPアドレス	サブネットマスク	デフォルトゲートウェイ	VLANモード		
1	有効	Ethernet(自動)	192.168.0.3	255.255.255.0	192.168.0.1	タグなし	編集	再取得
2	有効	Ethernet(固定)	192.168.0.5	255.255.255.0	192.168.0.1	シングルタグ	編集	再取得
3	無効	Ethernet(自動)	---.---.---.---	---.---.---.---	---.---.---.---	タグなし	編集	再取得

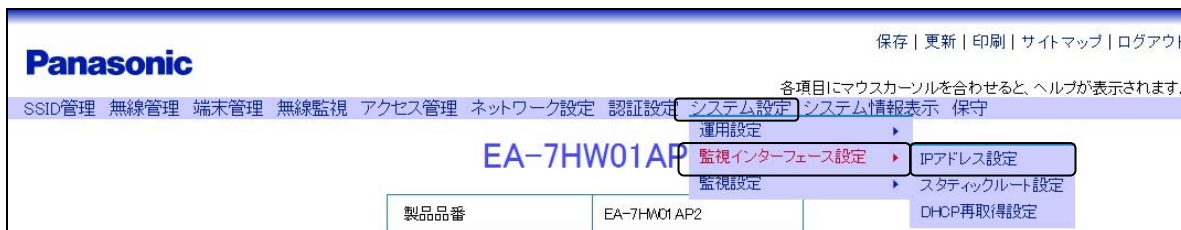
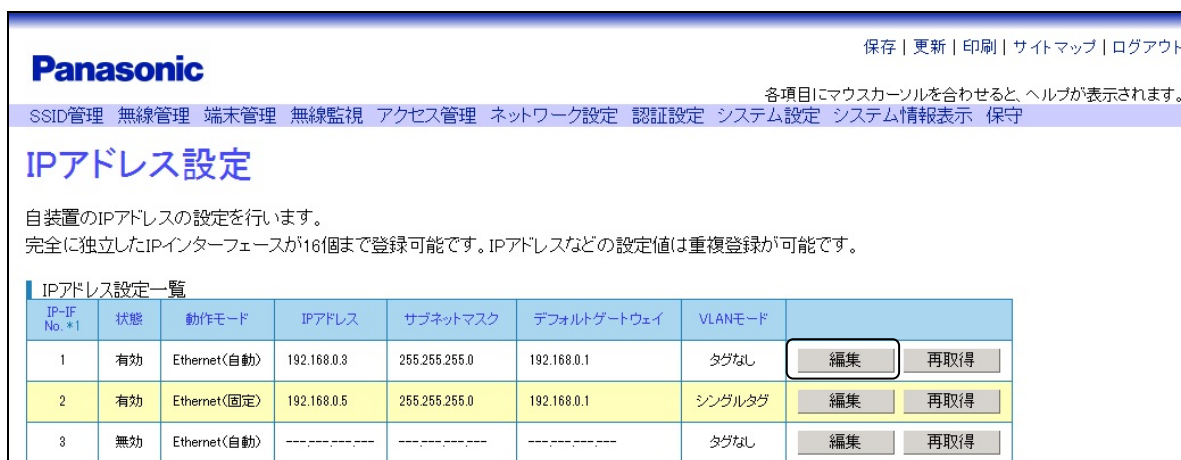



図5.2-4　IP アドレス設定

手順 3 ～ 手順 4 は〔IP アドレス編集〕画面（図 5.2-5）より各種設定を行います。

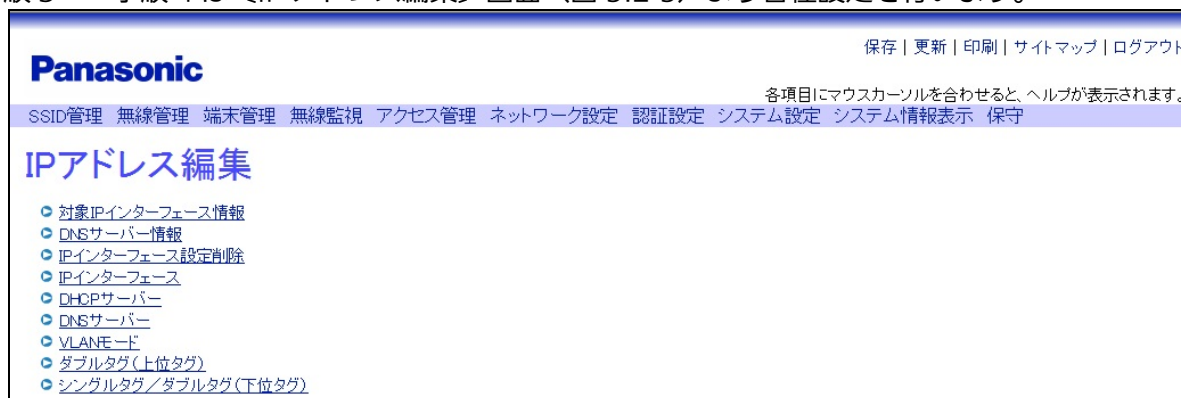



図5.2-5　IP アドレス編集

手順3　〔IP アドレス編集〕画面（図 5.2-5）の〔IP インターフェース〕をクリックし、
IP インターフェース 1 番に対して下記設定を行います。

- インターフェースの〔有効〕を選択
- 動作モードの〔Ethernet（固定)〕を選択
- IP アドレスに「192.168.12.11」を入力
- サブネットマスクに「255.255.255.0」を入力
- デフォルトゲートウェイに「192.168.12.254」を入力

図5.2-6　IP インターフェース設定（屋内用無線 LAN アクセスポイント）

図5.2-7　IP インターフェース設定（屋外用無線 LAN アクセスポイント）

手順4　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

◆装置設定

手順5　〔システム設定〕　→　〔運用設定〕　→　〔装置設定〕を選択します。

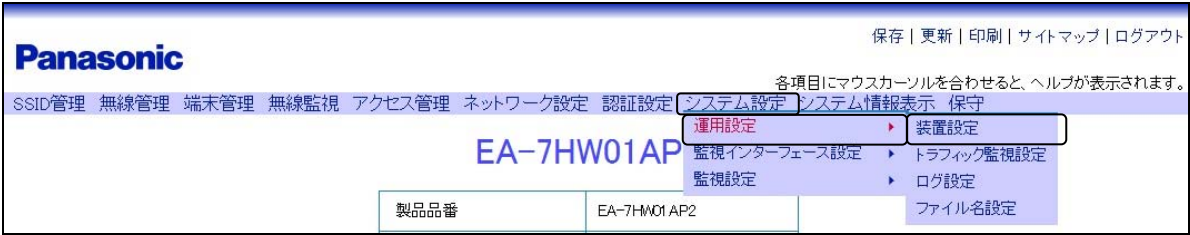



図5.2-8　メニュー（装置設定）

手順6　〔装置情報〕をクリックします。

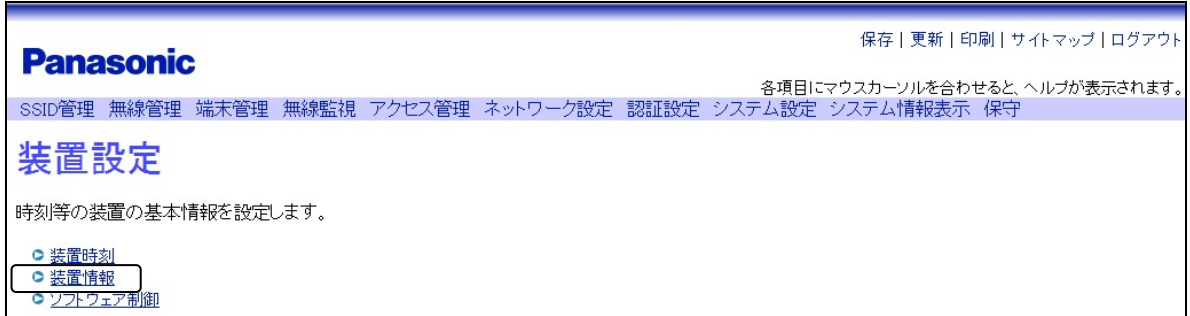



図5.2-9　装置設定

手順7　装置名称を入力します。
（入力は、半角英数字または半角記号（[?] は除く）　0～255 文字以内で行ってください。）
「装置名称（SysName)」は、L2TP 設定の自装置ホスト名となります。

図5.2-10　装置情報

手順8　装置情報下部の〔設定〕ボタンを押し、設定を反映させます。

◆IPsec 設定

手順9　〔ネットワーク設定〕　→　〔IPsec 設定〕を選択します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守
Ethernetポート設定
ポート-VLANマッピング
VLAN-L2TPマッピング
L2TP設定
PPP設定
IPsec設定
リンクパススルー
LTE/3G設定

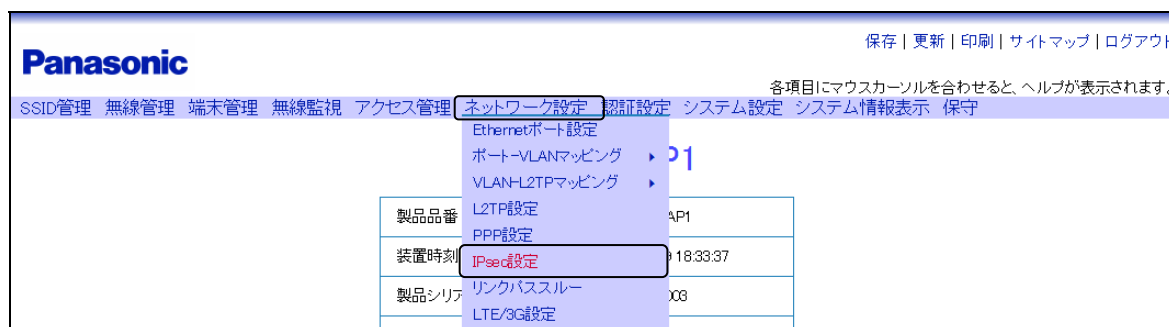



図5.2-11　ネットワーク設定（IPsec 設定　屋内用無線 LAN アクセスポイント）

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守
Ethernetポート設定
ポート-VLANマッピング
VLAN-L2TPマッピング
L2TP設定
PPP設定
IPsec設定
リンクパススルー

図5.2-12　ネットワーク設定（IPsec 設定　屋外用無線 LAN アクセスポイント）

手順 10 ～ 手順 15 は〔IPsec 設定〕画面（図 5.2-13）より各種設定を行います。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

IPsec設定

IPsecに関する詳細設定を行います。

- IPsec設定表示
- IKE状態表示
- IPsec状態表示
- IPsec設定
- コネクション先IP設定
- 自装置証明書パスワード登録
- 相手先認証方式
- 事前共有秘密鍵設定
- IKE SA生存時間
- IPsec SA生存時間
- ローカルID設定

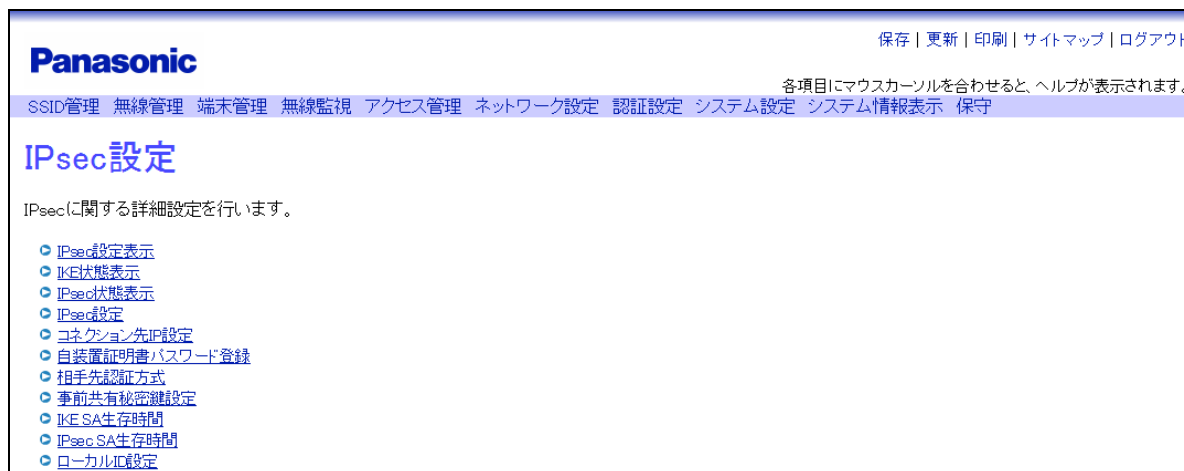



図5.2-13　IPsec 設定

手順10　〔IPsec 設定〕画面（図 5.2-13）の〔IPsec 設定〕をクリックし、〔有効〕を選択します。

図5.2-14　IPsec 設定の有効／無効

手順11　〔IPsec 設定〕画面（図 5.2-13）の〔コネクション先 IP 設定〕をクリックし、下記内容を設定します。

- 自装置 IP エントリー番号の“1”を選択
- コネクション先 IP アドレスに「192.168.11.252」を入力

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
コネクション先IP設定
自装置IPエントリ番号 *1　1
コネクション先IPアドレス *1　192.168.11.252　(XXX.XXX.XXX.XXX [XXX=0～255])

図5.2-15　コネクション先 IP 設定

手順12　〔IPsec 設定〕画面（図 5.2-13）の〔自装置証明書パスワード登録〕をクリックし、「Pass5678」を入力します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
自装置(自局)証明書パスワード登録(PKCS#12)
パスワード *2 *3　Pass5678
入力確認

図5.2-16　自装置（自局）証明書パスワード登録(PKCS#12)

手順13　〔IPsec 設定〕画面（図 5.2-13）の〔相手先認証方式〕をクリックし、〔RSASIG〕を選択します。

図5.2-17　相手先認証方式

手順14　〔IPsec 設定〕画面（図 5.2-13）の〔ローカル ID 設定〕をクリックし、〔IP アドレス、または、公開鍵証明書のサブジェクト〕を選択します。

図5.2-18　ローカル ID 設定

手順15　画面最下部の〔設定〕ボタンを押し、設定を反映させます。

以下、「5.1　L2TP over PPPoE ネットワーク接続での設定」の手順 12 ～ 手順 20（◆L2TP 設定）をご参照ください。

重要	■ IPsec を認証方式＝DSS、RSASIG で接続する場合は、あらかじめ各種証明書を FTP または TFTP で本装置に put しておく必要があります。 ■ DSS、RSASIG では、対向装置と本装置の時刻がずれていた場合、接続が失敗する恐れもありますのでご注意ください。

5.3　LTE/3G接続を利用してのインターネットVPN接続（屋内用無線LANアクセスポイントのみ）

ここでは、本装置（屋内用無線 LAN アクセスポイント：EA-7HW01AP1 のみ）にて LTE/3G を利用して L2TP に IPsec を併用することでデータの機密性や完全性を確保した VPN 接続を行い、無線 LAN 端末データの転送を実現するための基本的な設定方法を説明します。
なお、L2TP、IPsec 接続先装置の設定については、設置機器の装置マニュアルを別途参照してください。

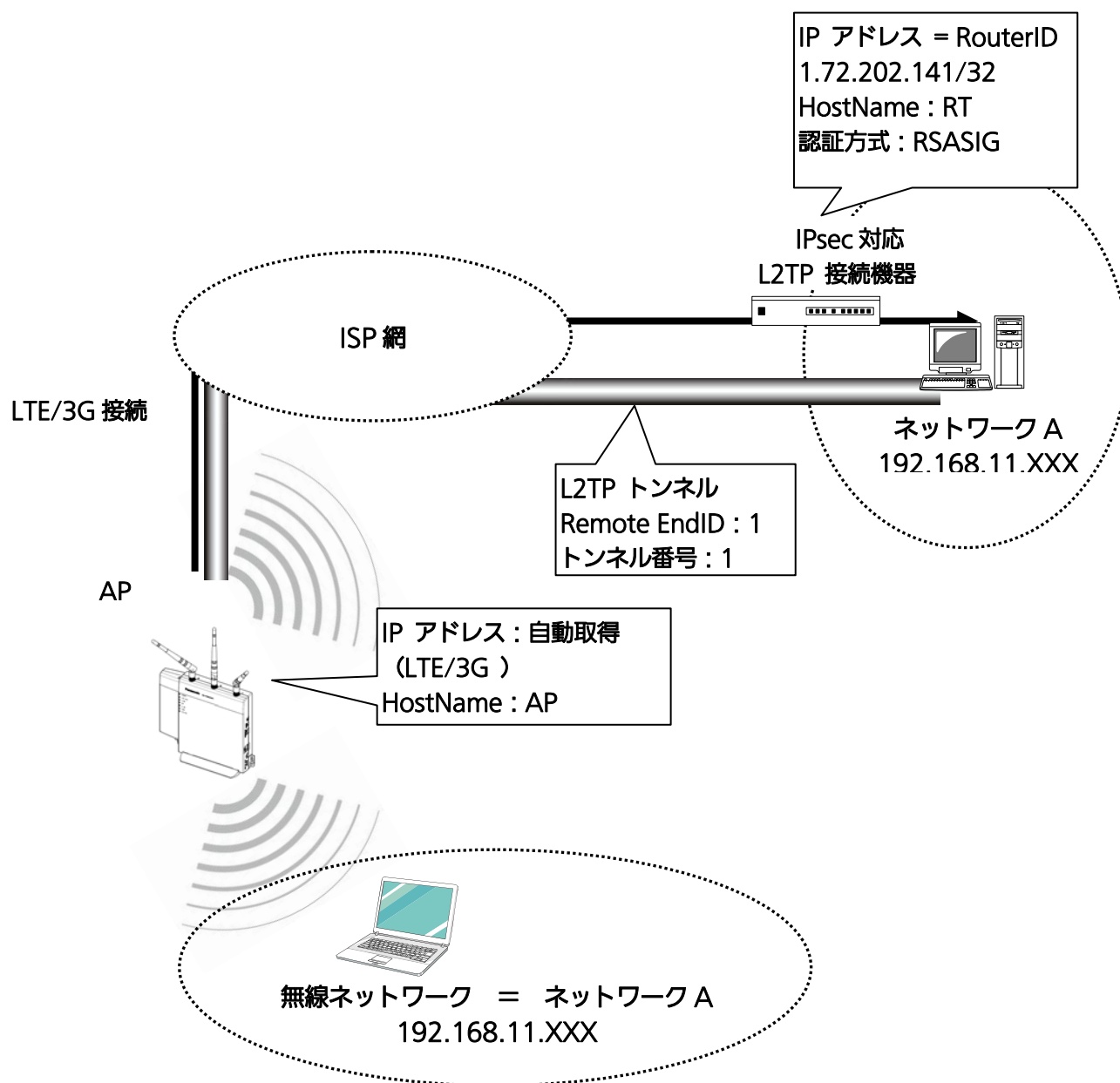



図5.3-1　LTE/3G 接続イメージ

図 5.3-1（LTE/3G を利用しての L2TP over IPsec）を構築するための設定は、以下の手順で行います。

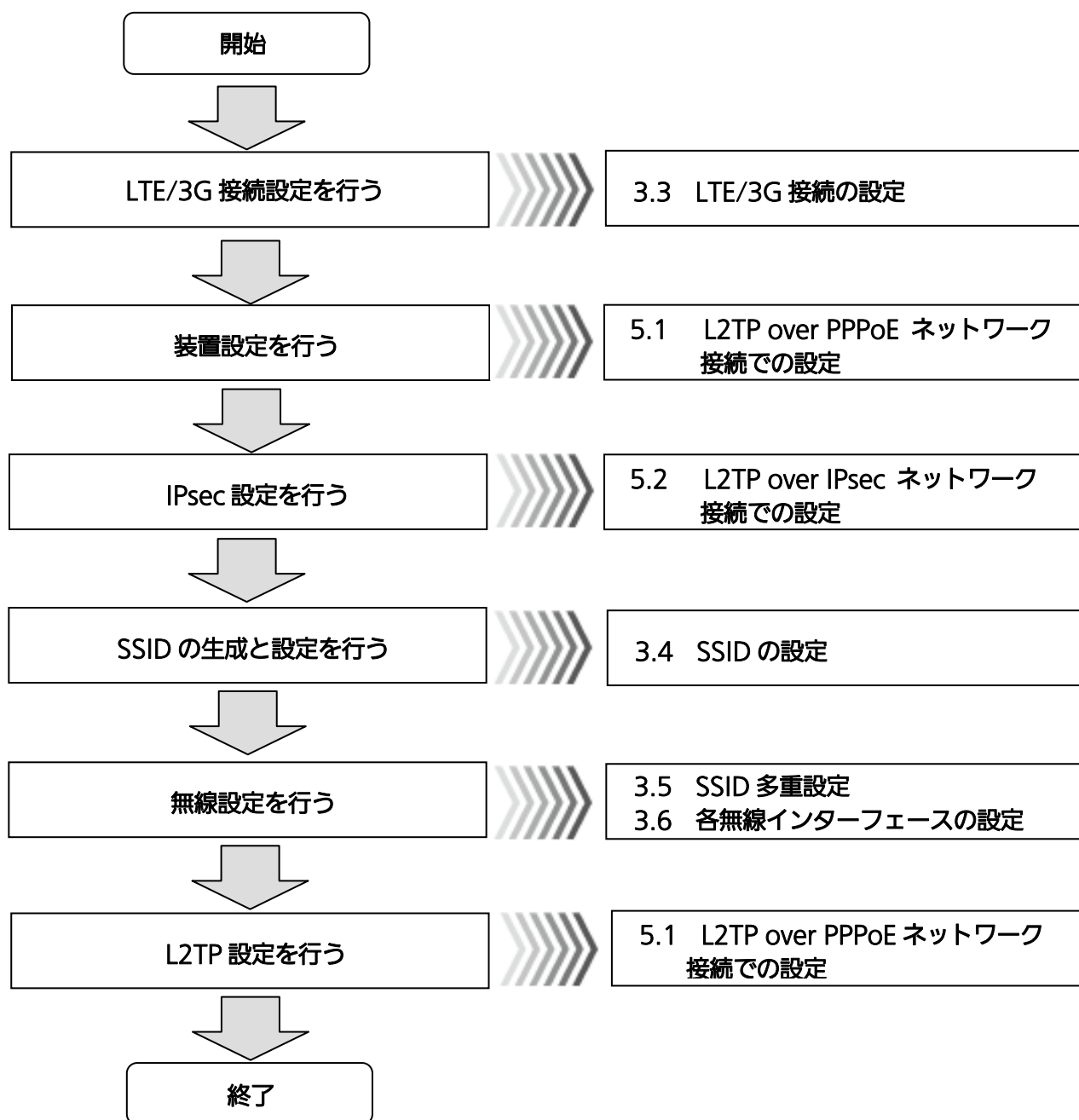



図5.3-2 ネットワーク構成手順（LTE/3G 接続を利用しての L2TP over IPsec）

設定手順

◆IP アドレス設定

「3.3　LTE/3G 接続の設定」の手順 1 ～ 手順 22 をご参照ください。

◆装置設定

「5.1　L2TP over PPPoE ネットワーク接続での設定」の手順 5 ～ 手順 8 をご参照ください。

◆IPsec 設定

「5.2　L2TP over IPsec ネットワーク接続での設定」の手順 9 ～ 手順 15 をご参照ください。

◆SSID の生成と設定

「3.4　SSID の設定」 - 「◆SSID の生成」の手順 1 ～ 手順 3 および「3.4　SSID の設定」 - 「◆SSID の設定」の手順 1 ～ 手順 10 をご参照ください。

◆無線設定

「3.5　SSID 多重設定」 - 「◆SSID 多重での SSID 動作設定」の手順 1 ～ 手順 5 および「3.6　各無線インターフェースの設定」 - 「◆無線インターフェースの設定」の手順 1 ～ 手順 4 をご参照ください。

◆L2TP 設定

「5.1　L2TP over PPPoE ネットワーク接続での設定」の手順 12 ～ 手順 20（◆L2TP 設定）をご参照ください。

重要	■ LTE/3G 接続を利用して IPsec 接続する場合、本装置で LTE 再接続により IP アドレスが変わると対向装置で設定変更が必要になります。IP アドレス変更時に対向装置での設定変更を不要にするには、IPsec 設定にて以下のいずれかに設定してください。 (1) 相手先認証方式として DSS または RSASIG を設定し、ローカル ID 設定を IP アドレス、または、公開鍵証明書のサブジェクトに設定 (2) 相手先認証方式として PSK を設定する場合は、ローカル ID 設定の ID 種別を FQDN、FQDN に値を設定

5.4　リンクパススルー設定

本装置では、WAN 側のリンク切断に連動して、無線機能を閉塞にするリンクパススルー機能があります。無線機能閉塞時には、接続中の端末や MAC ブリッジ接続を切断します。
また、リンクパススルー実行後は、WAN 側の接続を検出するまで、無線機能の閉塞を継続します。

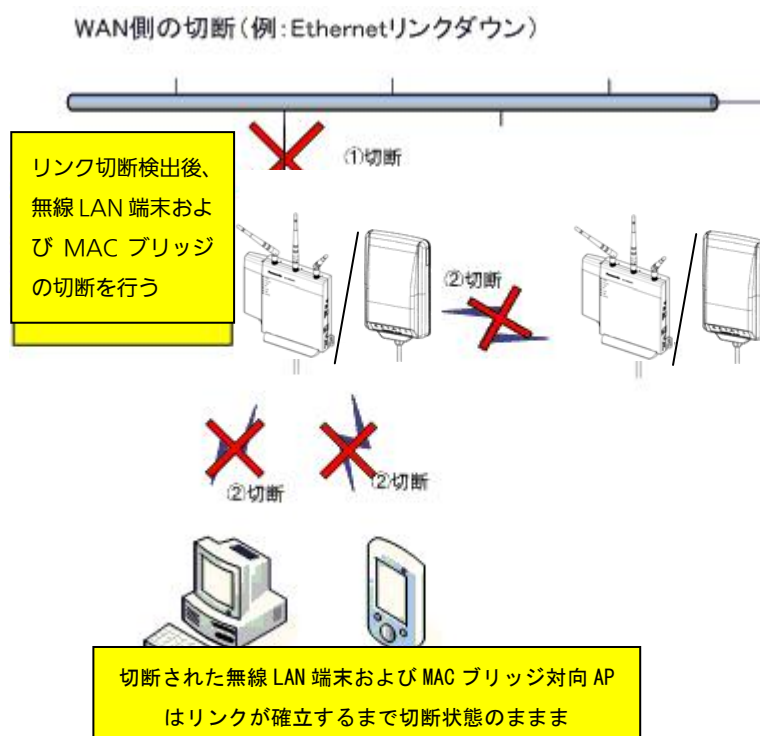



図5.4-1　リンクパススルー概要

No.	WAN	判断基準	監視対象
1	LTE/3G	LTE/3G として使用する（PPP モードが LTE/3G かつ IP 動作モードが PPP）自装置 IP エントリがある場合	①LTE/3G 接続状態②L2TP トンネルの接続状態※1※2 ③IPsec トンネルの接続状態※1
2	MAC ブリッジ	無線インターフェースのどちらかが MAC ブリッジクライアントの場合	①MAC ブリッジの接続状態
3	Ethernet	上記以外	①Ethernet のリンク状態 ②L2TP トンネル状態※3 ③IPsec トンネルの接続状態

※1：L2TP と IPsec の接続状態は、トンネルに使用している自装置 IP エントリと、LTE/3G として使用している（PPP モードが LTE かつ IP 動作モードが PPP）自装置 IP エントリが同じトンネルのみ対象とします。
※2：LTE/3G として使用している自装置 IP エントリ番号と同じ自装置 IP エントリ番号のトンネルが複数ある場合は、ひとつでもトンネルが切断された場合に、リンク切断と判断します。
※3：Ethernet として使用している自装置 IP エントリ番号と同じ時装置 IP エントリ番号の有効なトンネルが複数ある場合は、ひとつでもトンネルが切断された場合に、リンク切断と判断します。

操作手順

手順1　〔ネットワーク設定〕　→　〔リンクパススルー〕を選択します。

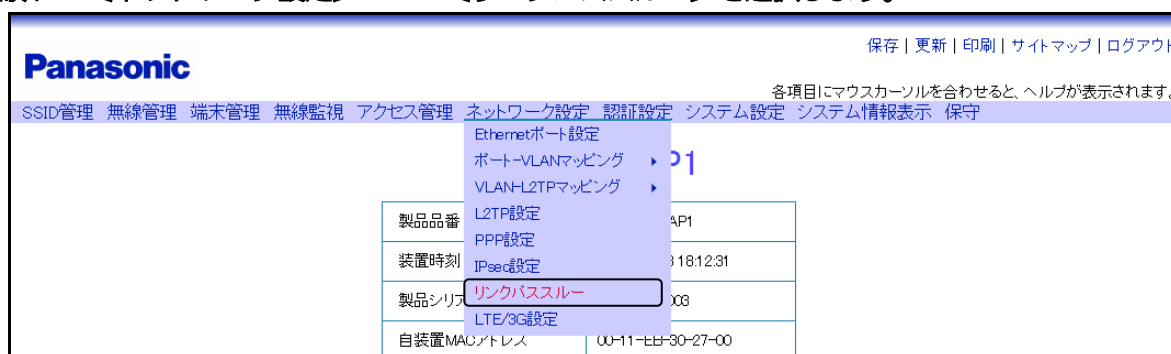



図5.4-2　メニュー（リンクパススルー　屋内用無線 LAN アクセスポイント）

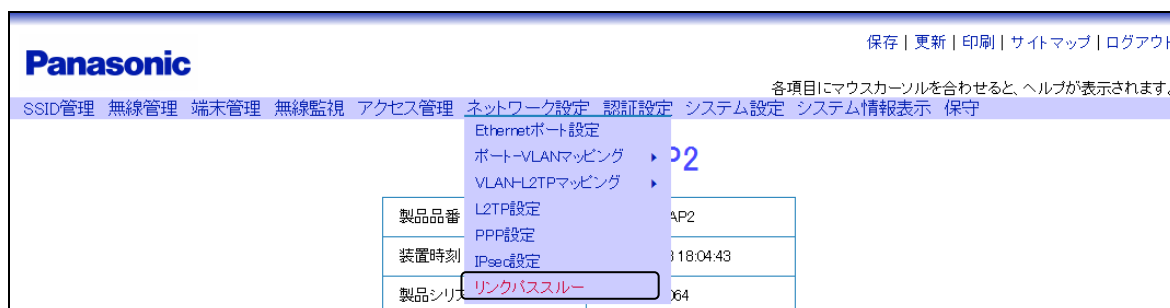



図5.4-3　メニュー（リンクパススルー　屋外用無線 LAN アクセスポイント）

手順 2 ～ 手順 4 は〔リンクパススルー〕画面（図 5.4-4）より各種設定を行います。

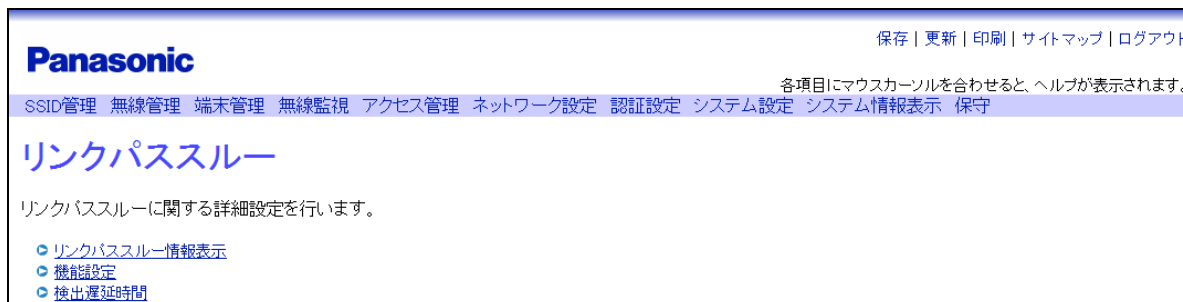



図5.4-4　リンクパススルー

手順2　〔リンクパススルー〕画面（図 5.4-4）の〔機能設定〕をクリックし、リンクパススルー設定の有効をクリックしチェックします。

(※リンクパススルーを無効にする場合は無効にチェックします)

図5.4-5　機能設定

手順3　検出遅延時間の遅延時間を入力します。

例として 45 秒に設定します。

※検出遅延時間は、WAN 側の切断検出から、リンクパススルー機能（無線機能の閉塞）が動作するまでの時間の時間です。設定時間内に WAN 側のリンクが確立した場合は、リンクパススルー機能は動作しません。

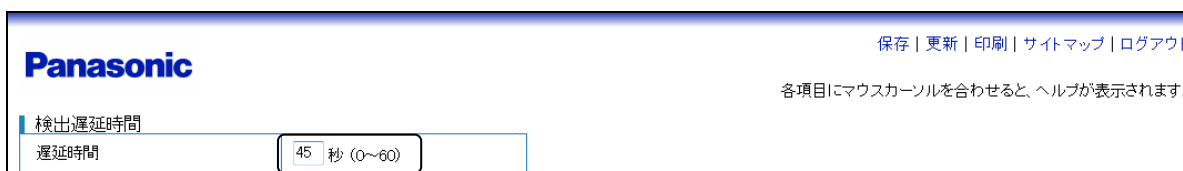



図5.4-6　検出遅延時間

手順4　画面最下部の〔設定〕ボタンをクリックし、設定を反映させます。

第６章　保守

本装置の保守機能（ログ機能、アップロード・ダウンロード、装置リセットなど）について、説明します。

6.1　設定データのバックアップと読み込み

6.1.1　設定データのバックアップ

本装置の設定データをバックアップする方法は、FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法、CLI コンソールでコマンドを実行する方法があります。ここでは、FTP コマンドを使用して、本装置に接続している PC に設定ファイルをバックアップする方法を紹介します。一部の設定は設定データでバックアップできないため、全設定をバックアップしたい場合は、全設定一括バックアップをご利用ください。

操作手順

手順1　〔システム設定〕　→　〔運用設定〕　→　〔ファイル名設定〕を選択します。

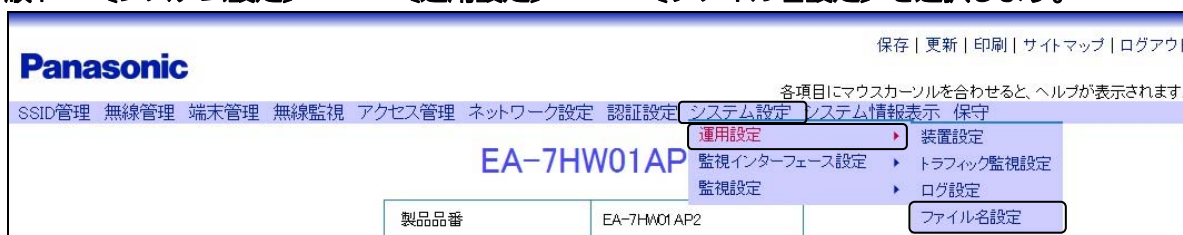



図6.1-1　メニュー（ファイル名設定）

手順2　設定ファイルのファイル名を入力します。（拡張子は不要）

例として、「setting」を入力します。
ここで設定したファイル名が、バックアップファイル名となります。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

ファイル名設定

自装置の各種ファイルを制御する際に使用するファイル名を設定します。
ファイル名は、半角英数字またはアンダーライン(_)・ハイフン(-)・ピリオド(.) 0～31文字以内で入力してください。

ファイル名設定

自装置ファームウェア(1面)	firmware1
自装置ファームウェア(2面)	firmware2
設定ファイル	setting
イベントログファイル	eventlog

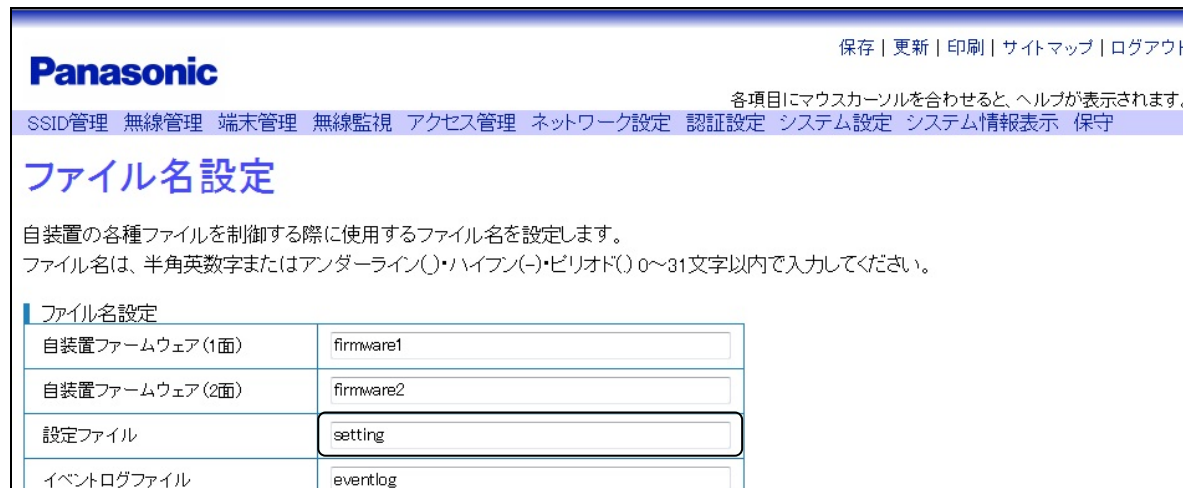



図6.1-2　ファイル名設定

手順3　画面最下部の〔設定〕ボタンをクリックし、設定を反映させます。

手順4　Windows の〔スタート〕ボタンをクリックし、〔すべてのプログラム〕
→　〔アクセサリ〕　→　〔コマンド プロンプト〕をクリックします。

手順5　〔コマンドプロンプト〕画面が表示されたら、バックアップした設定データを保存したいディレクトリへ移動します。

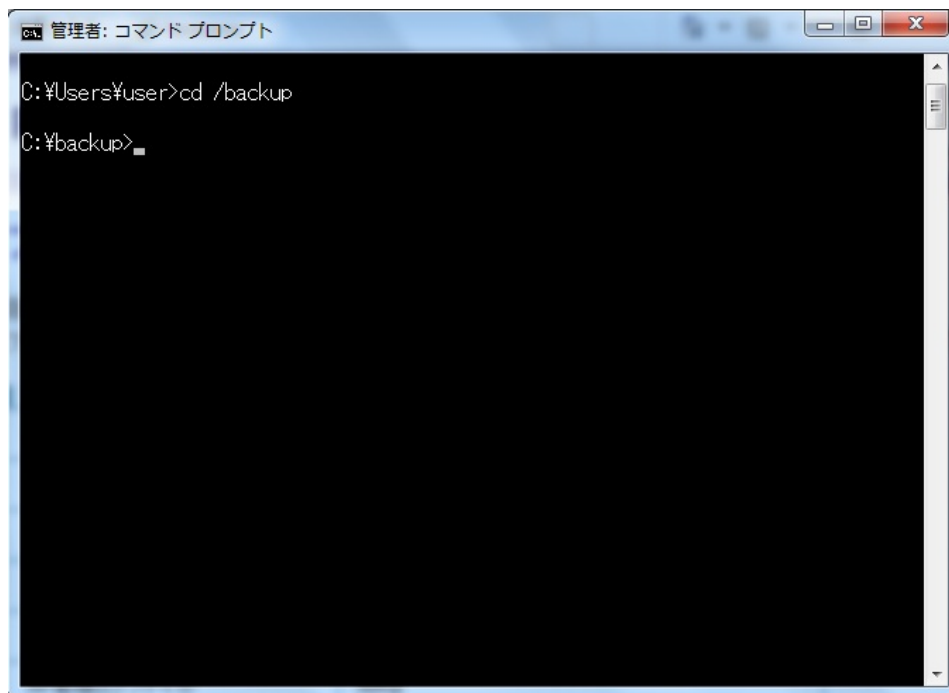



図6.1-3　設定ファイルバックアップ（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC から本装置に接続します。
本装置の IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

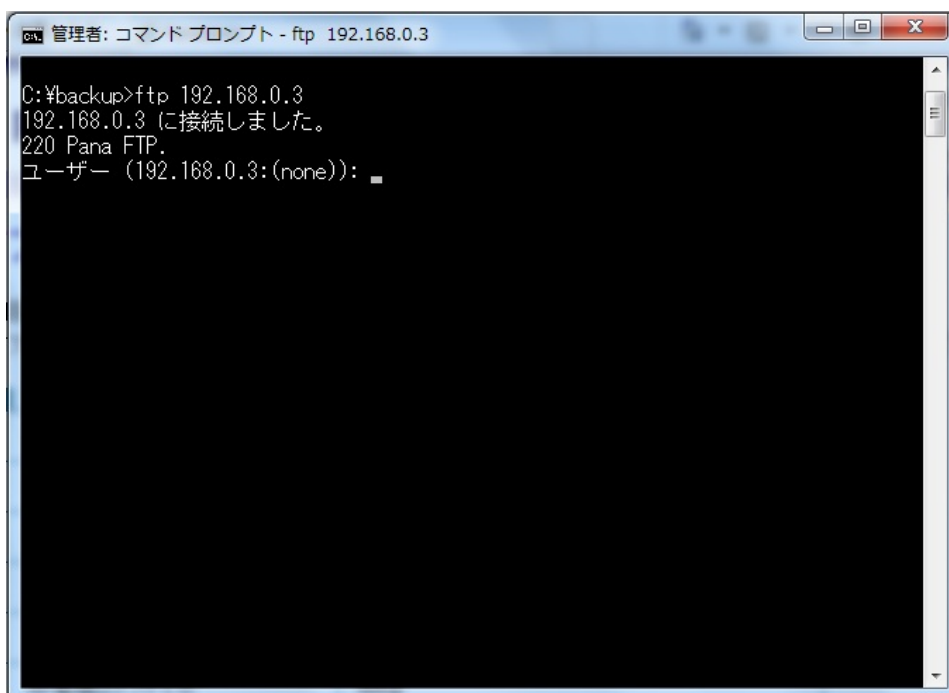



図6.1-4　設定ファイルバックアップ（コマンド）②

※「ftp 192.168.0.3」と実行してもユーザー名の入力が表示されず「ftp>」と表示された場合は、CLI コンソールから以下のコマンドを実行してください。

```
# ftp access off

# ftp access on

#
```

「5.1.2　設定データの読み込み」、「6.1.3　全設定一括バックアップ」、「6.1.4　全設定一括読み込み」、「6.2　ファームウェアのアップデート」の場合も同様に、ユーザー名の入力が表示されず「ftp>」と表示された場合は、CLI コンソールから上記のコマンドを実行してください。

手順7　パスワードを入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

図6.1-5　設定ファイルバックアップ（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful.」と表示されます。

図6.1-6　設定ファイルバックアップ（コマンド）④

手順9　設定ファイルをバックアップします。

ここでは、設定ファイルのファイル名を「setting」として、下記コマンドを入力／実行します。

コマンド： “get setting”

図6.1-7　設定ファイルバックアップ（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

図6.1-8　設定ファイルバックアップ（コマンド）⑥

※Windws XP では、tftp コマンドでの設定ファイルバックアップも可能です。

6.1.2　設定データの読み込み

本装置で設定データを読み込む方法は、本装置に接続している PC より FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法があります。ここでは、FTP コマンドを使用して本装置に接続している PC より本装置へ設定ファイルを読み込む方法を紹介します。

操作手順

手順1　～　手順 4 は、「6.1.1　設定データのバックアップ」を参照してください。

手順5　保存している設定データのディレクトリへ移動します。

ここでは、「C:\backup」に「setting」という名称の設定ファイルを保存しているものとします。

図6.1-9　　設定ファイル読み込み（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC から本装置に接続します。

本装置の IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

```
管理者: コマンド プロンプト - ftp  192.168.0.3

C:¥backup>ftp 192.168.0.3
192.168.0.3 に接続しました。
220 Pana FTP.
ユーザー (192.168.0.3:(none)):
```

図6.1-10　　設定ファイル読み込み（コマンド）②

手順7　ユーザー名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

図6.1-11　設定ファイル読み込み（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful」と表示されます。

図6.1-12　設定ファイル読み込み（コマンド）④

手順9　設定ファイルを読み込みます。

ここでは、設定ファイルのファイル名を「setting」として、下記コマンドを入力／実行します。

コマンド：“put setting”

図6.1-13　設定ファイル読み込み（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

図6.1-14　設定ファイル読み込み（コマンド）⑥

※Windws XP では、tftp コマンドでの設定ファイル読み込みも可能です。

6.1.3　全設定一括バックアップ

本装置の全設定データを一括バックアップする方法は、FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法、CLI コンソールでコマンドを実行する方法があります。ここでは、FTP コマンドを使用して、WEB コンソールに接続している PC に設定ファイルをバックアップする方法を紹介します。

操作手順

手順1　〔システム設定〕　→　〔運用設定〕　→　〔ファイル名設定〕を選択します。

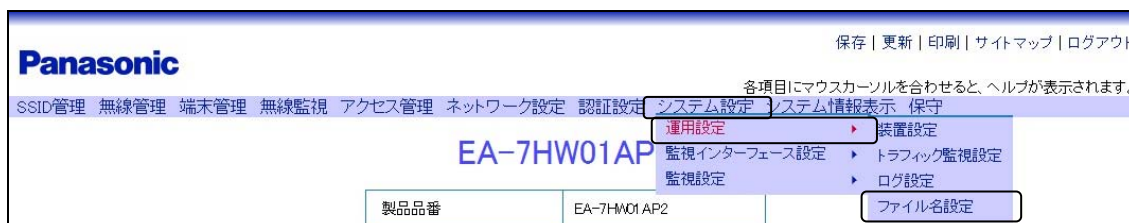



図6.1-15　メニュー（ファイル名設定）

手順2　設定ファイルのファイル名を入力します。（拡張子は不要）

例として、「allconfig」を入力します。
ここで設定したファイル名が、バックアップファイル名となります。

シーケンスログファイル	sequentiallog
干渉情報ログファイル	interferencelog
パケットログファイル	packetlog
統計情報ログファイル	statisticslog
認証局証明書ファイル名	cacert
自局証明書ファイル名	owncert
対向局公開鍵ファイル名	remotecert
認証局証明書失効リストファイル名	revocationlist
全設定ファイル	allconfig

このページのTopへ

設定

図6.1-16　ファイル名設定

手順3　画面最下部の〔設定〕ボタンをクリックし、設定を反映させます。

手順4　Windows の〔スタート〕ボタンをクリックし、〔すべてのプログラム〕
→　〔アクセサリ〕　→　〔コマンド プロンプト〕をクリックします。

手順5　〔コマンドプロンプト〕画面が表示されたら、バックアップした設定データを保存したいディレクトリへ移動します。

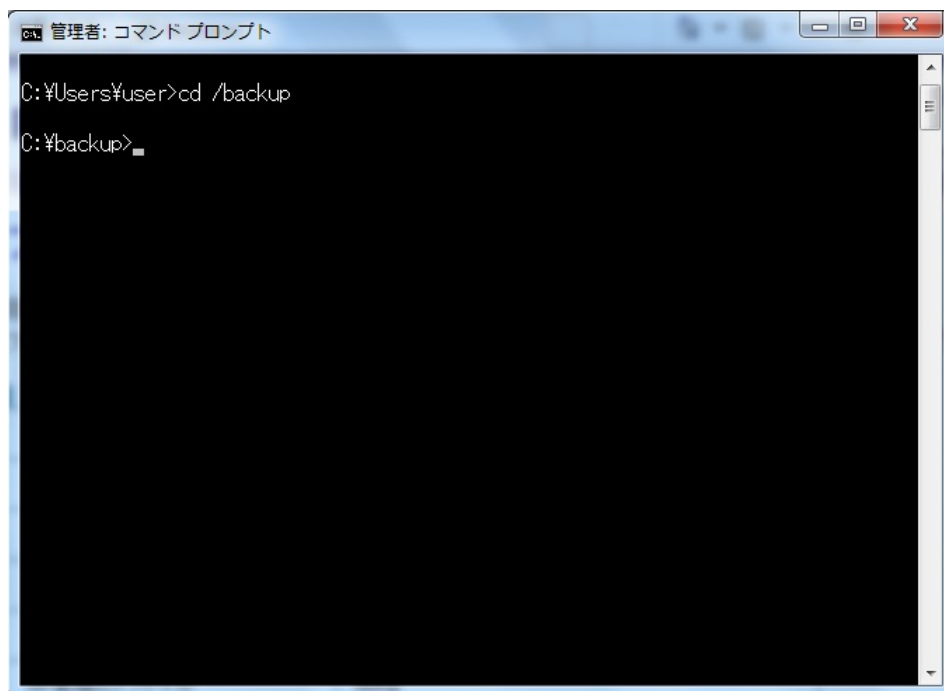



図6.1-17　全設定一括バックアップ（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC から本装置に接続します。

本装置の IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

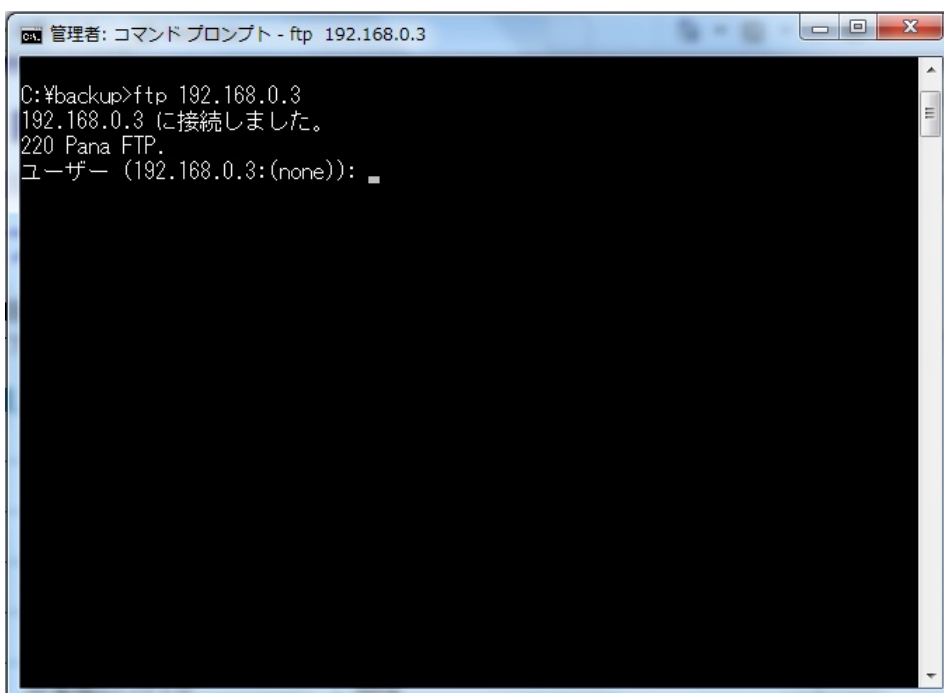



図6.1-18　全設定一括バックアップ（コマンド）②

手順7　ユーザー名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

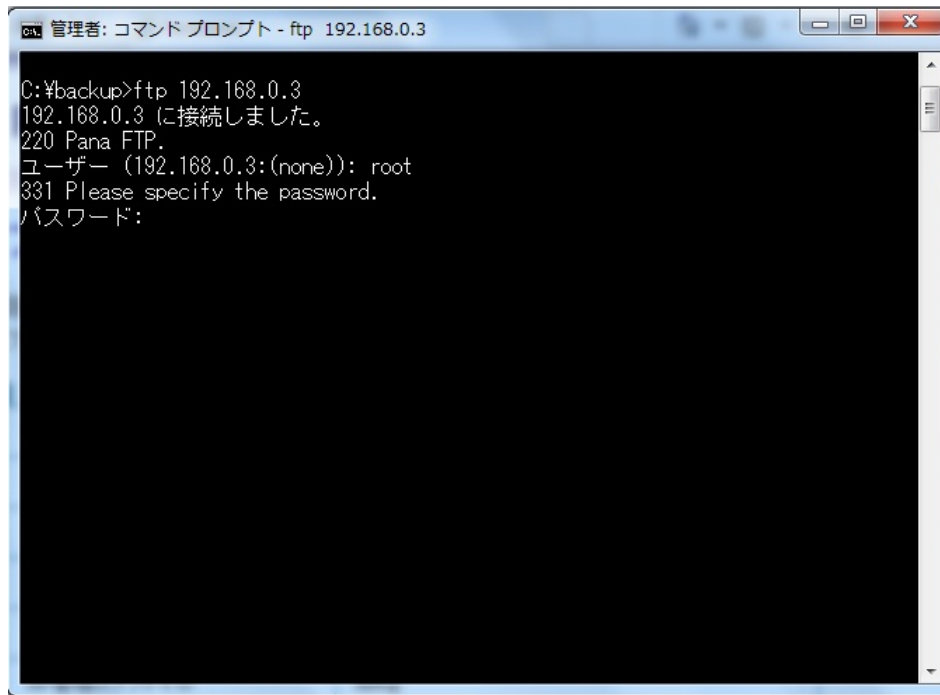



図6.1-19　全設定一括バックアップ（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful.」と表示されます。

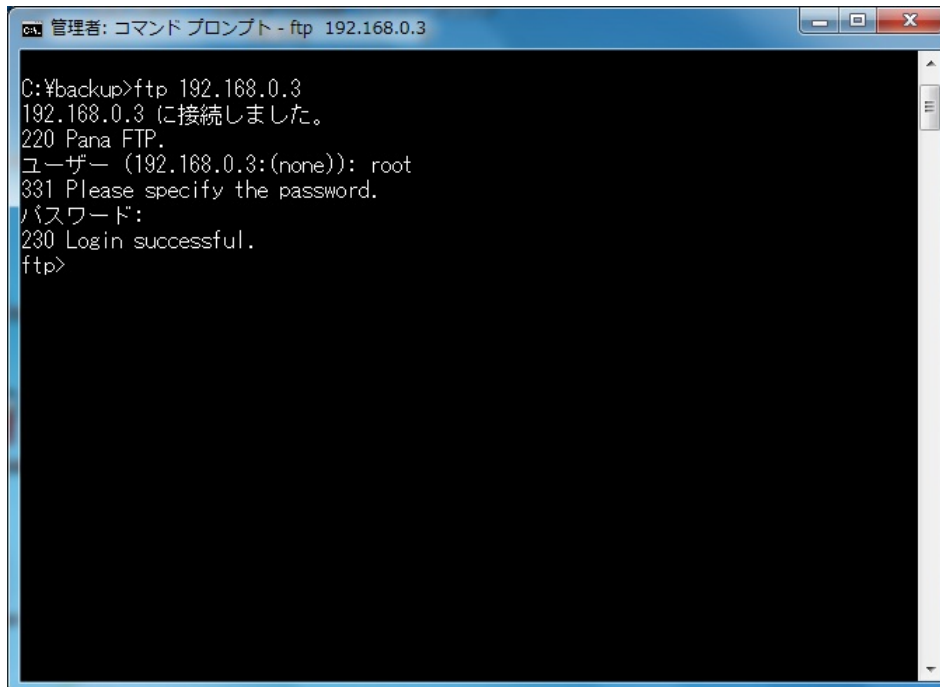



図6.1-20　全設定一括バックアップ（コマンド）④

手順9　設定ファイルをバックアップします。

ここでは、設定ファイルのファイル名を「allconfig」として、下記コマンドを入力／実行します。

コマンド：“binary”

コマンド：“get allconfig”

図6.1-21　全設定一括バックアップ（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

図6.1-22　全設定一括バックアップ（コマンド）⑥

※Windws XP では、tftp コマンドでの全設定一括バックアップも可能です。

6.1.4　全設定一括読み込み

本装置で全設定を一括で読み込む方法は、本装置に接続している PC より FTP コマンドを使用する方法、WEB コンソールでファイルコピーを使用する方法があります。ここでは、FTP コマンドを使用して本装置に接続している PC より本装置へ設定ファイルを読み込む方法を紹介します。

操作手順

手順1　～　手順 4 は、「6.1.3　全設定一括バックアップ」を参照してください。

手順5　保存している設定データのディレクトリへ移動します。

ここでは、「C:\backup」に「allconfig」という名称の設定ファイルを保存しているものとします。

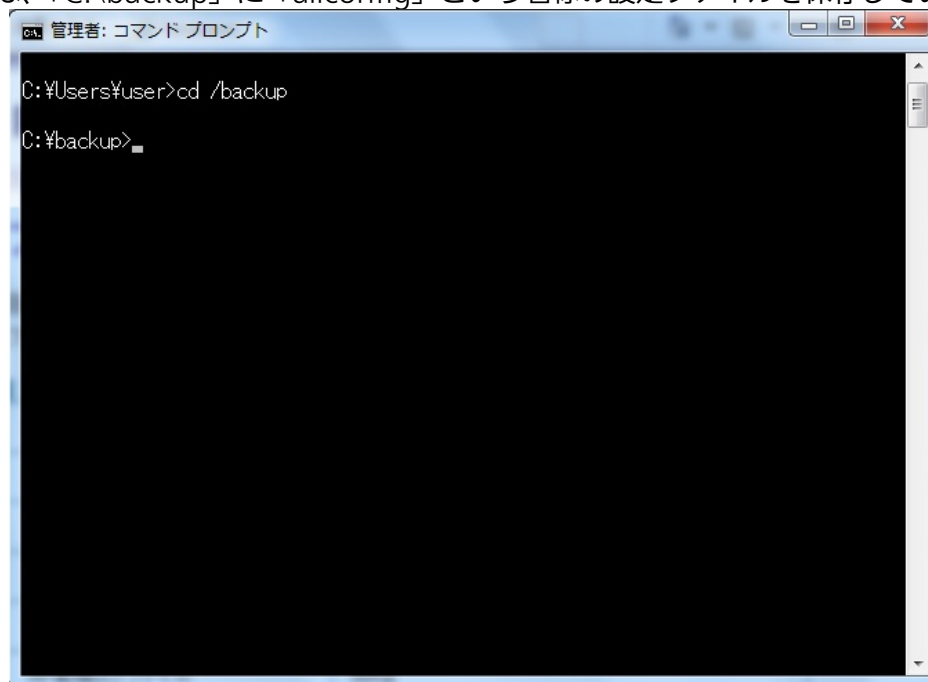



図6.1-23　全設定一括読み込み（コマンド）①

手順6　ftp コマンドを使って、WEB コンソール用 PC から本装置に接続します。

本装置の IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

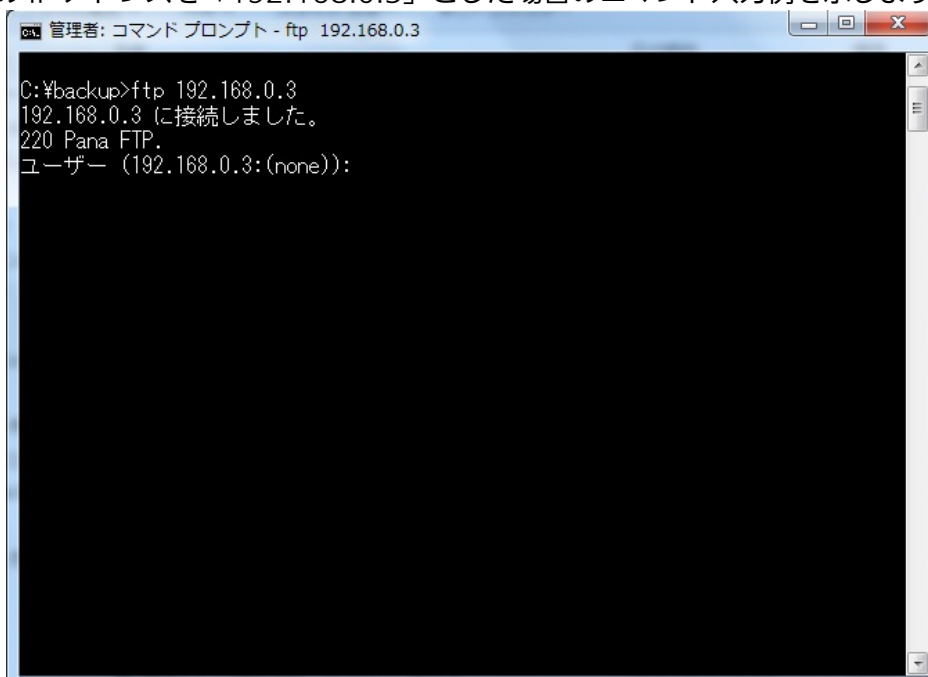



図6.1-24　全設定一括読み込み（コマンド）②

手順7　ユーザー名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

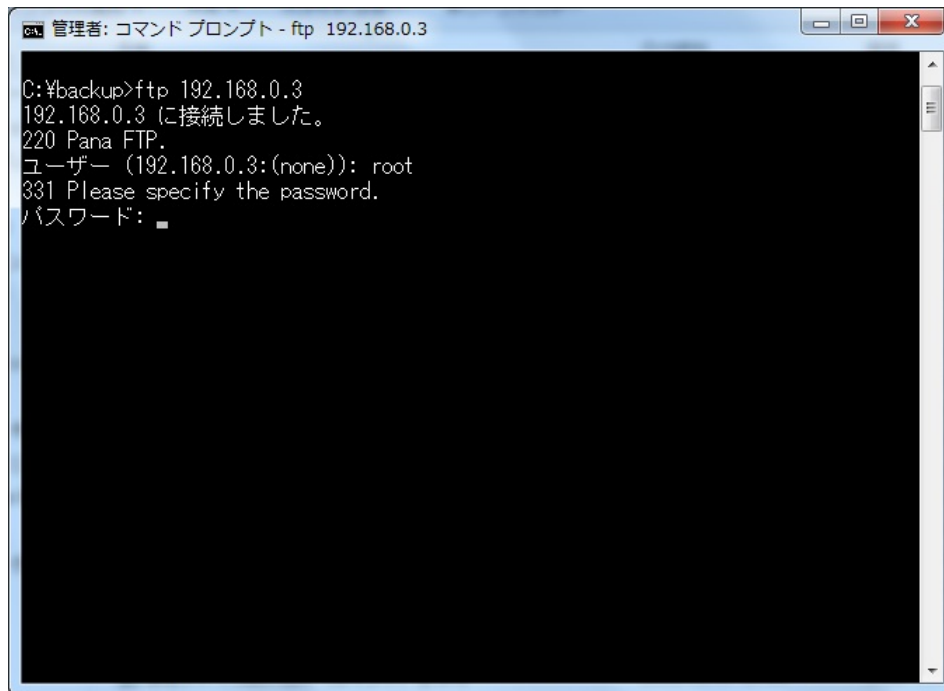



図6.1-25　全設定一括読み込み（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。
ログインが成功した場合は、「Login successful.」と表示されます。

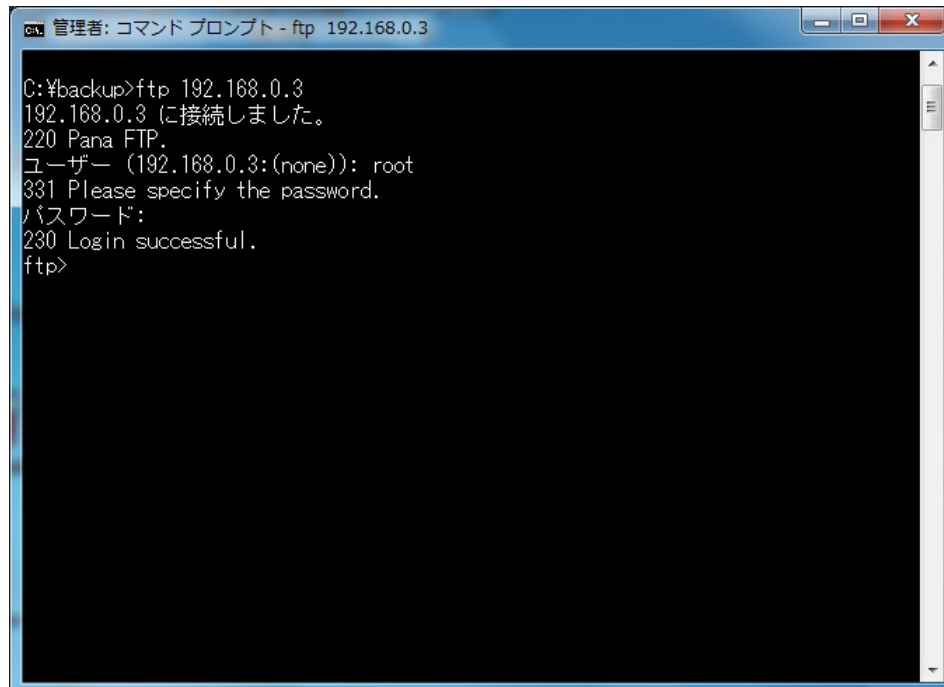
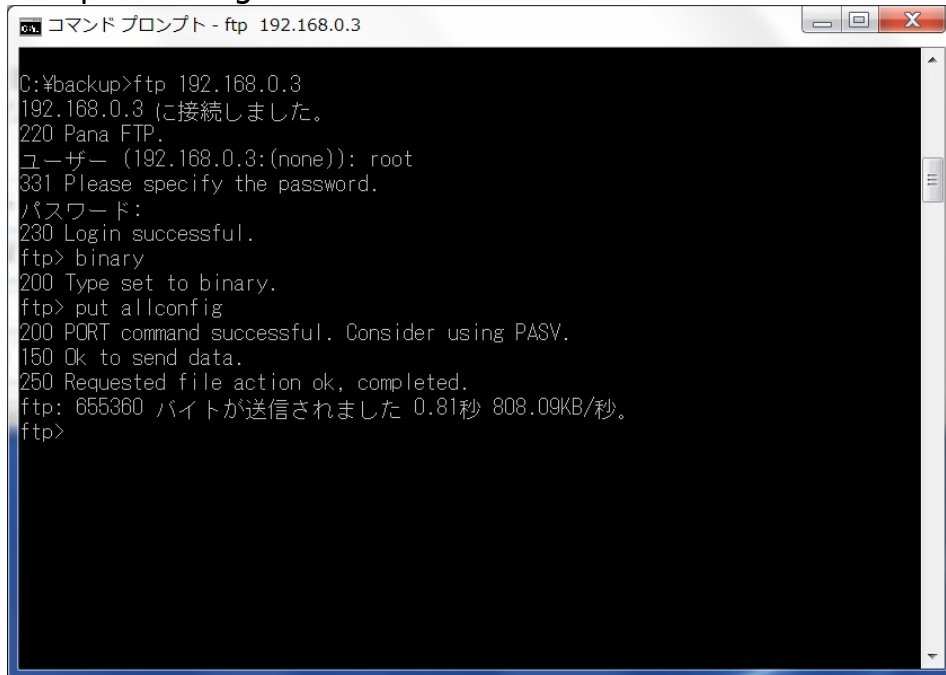
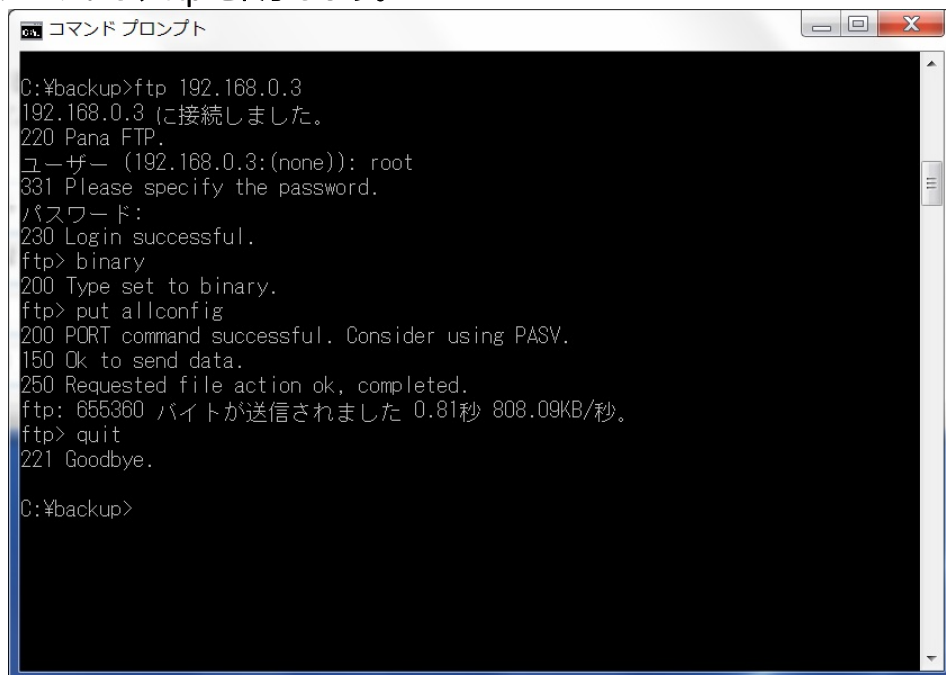



図6.1-26　全設定一括読み込み（コマンド）④

手順9　設定ファイルを読み込みます。

ここでは、設定ファイルのファイル名を「allconfig」として、下記コマンドを入力／実行します。

コマンド：“binary”

コマンド：“put allconfig”

```
コマンド プロンプト - ftp 192.168.0.3

C:¥backup>ftp 192.168.0.3
192.168.0.3 に接続しました。
220 Pana FTP.
ユーザー (192.168.0.3:(none)): root
331 Please specify the password.
パスワード:
230 Login successful.
ftp> binary
200 Type set to binary.
ftp> put allconfig
200 PORT command successful. Consider using PASV.
150 Ok to send data.
250 Requested file action ok, completed.
ftp: 655360 バイトが送信されました 0.81秒 808.09KB/秒。
ftp>
```

図6.1-27　全設定一括読み込み（コマンド）⑤

手順10　ログアウトし、ftp を終了します。

図6.1-28　全設定一括読み込み（コマンド）⑥

※Windws XP では、tftp コマンドでの全設定一括読み込みも可能です。

重要	全設定一括読み込みが完了した後、Web 画面もしくは CLI コンソール上から設定の保存を実行せずに、そのまま装置をリセットしてください。リセット前に設定の保存を実行すると、読み込んだ全設定が、現在起動中の設定で上書きされてしまいますのでご注意ください。

6.2　ファームウェアのアップデート

本装置では、手動にてファームウェアをアップデートすることができます。ファームウェアをアップデートする方法のひとつとして、FTP を利用する方法を紹介します。
ここでは、入手したファームウェアが、コンソールとして本装置に接続している PC に保存されているという前提で、本装置のファームウェアのアップデートを行います。

操作手順

手順1　〔システム設定〕 → 〔運用設定〕 → 〔ファイル名設定〕を選択します。

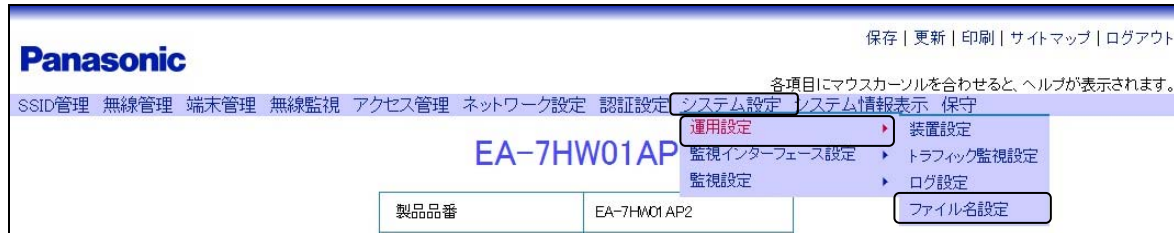



図6.2-1　メニュー（ファイル名設定）

手順2　読み込むファームウェアのファイル名を指定します。（拡張子は不要）
例として、自装置ファームウェア（1 面）に「apfirmware」を入力します。

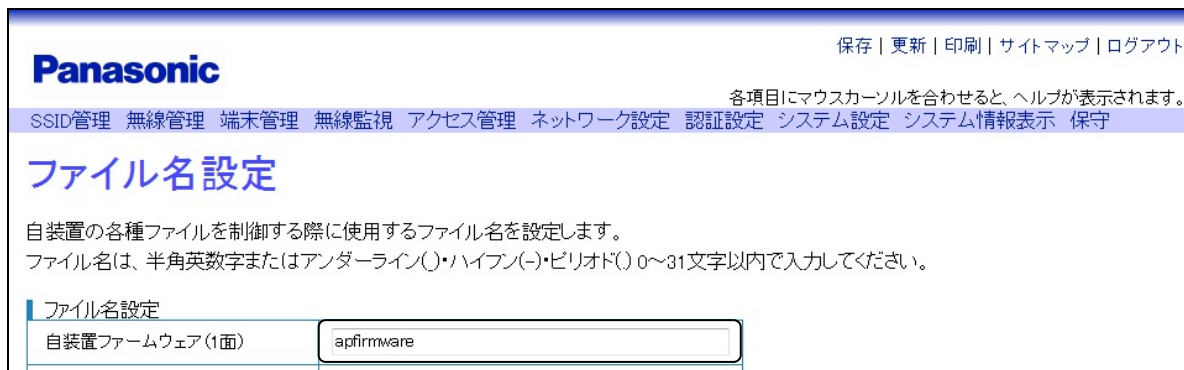



図6.2-2　ファイル名設定

手順3　画面最下部の〔設定〕ボタンをクリックし、設定を反映させます。
手順4　Windows の〔スタート〕ボタンをクリックし、〔すべてのプログラム〕
→ 〔アクセサリ〕 → 〔コマンド プロンプト〕をクリックします。

手順5　〔コマンドプロンプト〕画面が表示されたら、ファームウェアが保存されているディレクトリへ移動します。

ここでは、「C:\backup」に「apfirmware」という名称の設定ファイルを保存しているものとします。

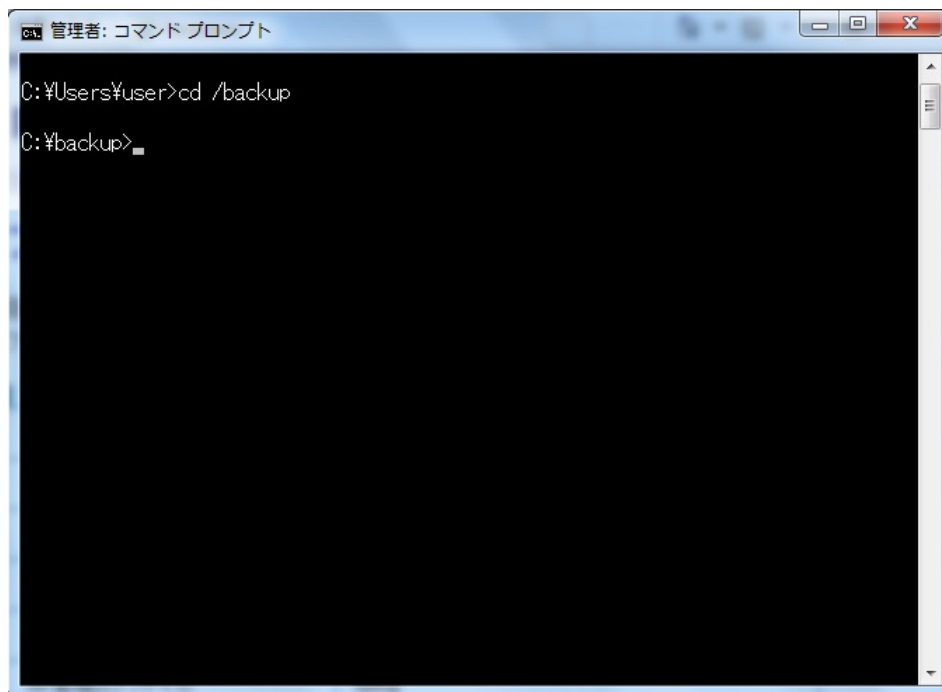



図6.2-3　ファームウェアのアップデート①

手順6　ftp コマンドを使って、WEB コンソール用 PC から本装置に接続します。

本装置の IP アドレスを「192.168.0.3」とした場合のコマンド入力例を示します。

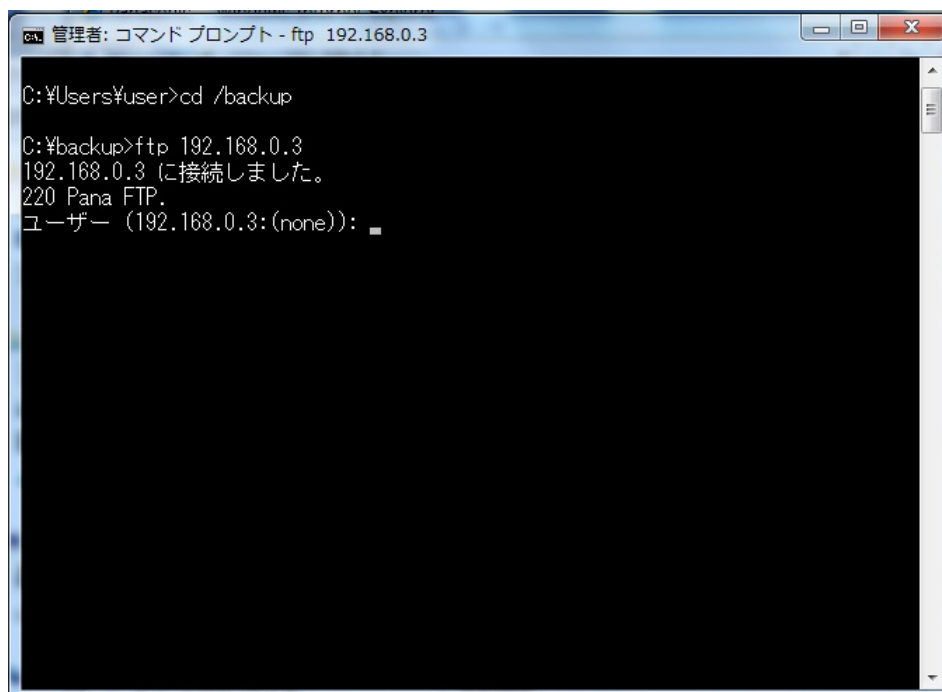



図6.2-4　ファームウェアのアップデート（コマンド）②

手順7　ユーザー名を入力し、実行します。

例として、管理者権限（ここでは初期値の「root」）を入力します。

図6.2-5　ファームウェアのアップデート（コマンド）③

手順8　パスワードを入力し、実行します。

パスワード入力時、画面に入力内容は表示されません。

ログインが成功した場合は、「Login successful.」と表示されます。

図6.2-6　ファームウェアのアップデート（コマンド）④

手順9　ftp コマンドを使って、本装置に接続中の PC よりファームウェアを読み込みます。

本装置の IP アドレスを「192.168.0.3」、アップデート用ファームウェアのファイル名を「apfirmware」
とした場合のコマンド入力例を示します。

コマンド：“put apfirmware”

図6.2-7　ファームウェアのアップデート⑤

手順 9 を実行後、ファームウェアのアップデート処理開始となります。

手順10　本装置をリセットし、読み込んだファームウェアを有効にします。

ftp の転送が完了した時点でファームウェアの更新は完了しています。本装置 のリセットを行ってください。

以上の操作により、ファームウェアのアップデートが完了となります。以下では、アップデートした
ファームウェアのバージョン確認方法を紹介します。

手順11 〔システム情報表示〕 → 〔ソフトウェア情報表示〕を選択します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守

ハードウェア情報表示
ソフトウェア情報表示
登録数表示
管理機能状態表示
ARP学習情報表示

EA-7HW01AP2

製品品番	EA-7HW01AP2
装置時刻	2000/01/01 00:15:02

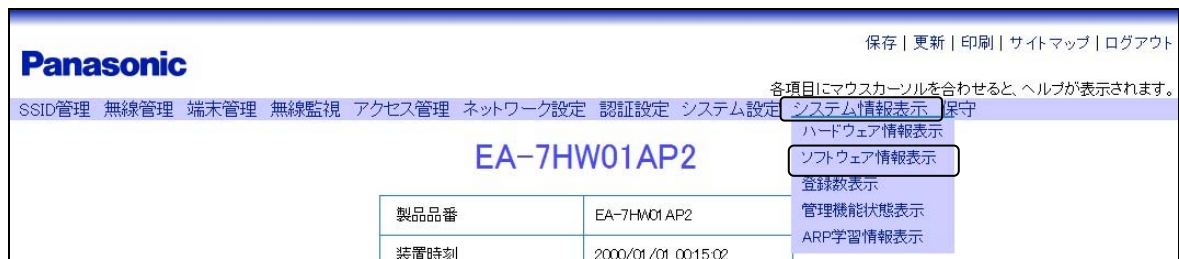



図6.2-8　メニュー（ソフトウェア情報表示）

手順12 アップデートしたファームウェアのバージョンを確認します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守

ソフトウェア情報表示

ソフトウェア情報

ブートROMバージョン	04.00
システムバージョン	01.00
起動中ファームウェアバージョン	04.01 Rev.0200
現在の起動ファームウェア面	1
リセット後起動ファームウェア面	1
ファームウェアバージョン(1面)	04.01 Rev.0200
ファームウェア作成日付(1面)	2013/04/03 14:34:00
ファームウェアバージョン(2面)	04.00 Rev.0300
ファームウェア作成日付(2面)	2013/02/07 15:18:00

図6.2-9　ソフトウェア情報表示

上記、手順 11 と手順 12 により、ファームウェアのバージョンを確認することができます。

6.3 ログ機能

本装置では、システムを運用管理するために有効なトラフィック統計情報や各種イベントなどをログデータとして蓄積し、コンソール上から表示、確認することができます。また、本装置内に蓄積されたログデータは、FTP（TFTP）サーバーに書き出すことが可能です。

※CLI コンソールでは、蓄積したログデータの読み出しには show コマンドを使用します。show コマンドについて詳しくは、コマンドリファンレスを参照してください。

6.3.1 ログ一覧

本装置が持つログデータの一覧を以下に示します。

表6.3-1　ログデータ一覧

モード名称	説明	データ保持	最大蓄積数
イベントログ	・セルフテスト結果 ・各種障害状態 ・AP 接続状態	電源 OFF 時ログデータ保持	512
AP 管理ログ	・AP 制御 ・AP 状態	電源 OFF 時ログデータ保持	512
端末管理ログ	・端末制御 ・端末状態 ・QoS 制御	保持なし	50,000
TRAP ログ	・Trap 送信	保持なし	256
アクセスログ	・Telnet アクセス ・TFTP アクセス ・FTP アクセス ・SNMP アクセス ・NTP アクセス ・HTTP アクセス　等	保持なし	512
設定ログ	・設定関係	保持なし	256
シーケンスログ	・Authentication ・Association ・Reassociation ・無線制御	保持なし	3072
干渉情報ログ	・周辺 AP の RSSI 値 ・ノイズフロア値	保持なし	786,432 （6Mbytes 分）
パケットログ	・管理フレーム ・認証フレーム	保持なし	500,000 （128Mbytes 分）
統計情報ログ	・端末接続台数 ・端末接続拒否回数	保持なし	180,000 （約　16Mbytes 分）

※　「電源 OFF 時ログデータ保持」となっているログは、10 分毎、またはリセット実施時に揮発領域から不揮発性領域に書き込み保存します。電源断をした場合は、不揮発性領域に保存後の 10 分間のデータ（不揮発性領域に保存される前の揮発性領域のデータ）は補償されません。

※　WEB コンソール・CLI コンソール・コマンドプロンプトでの FTP（TFTP）を使用して、ログ読出しが可能です。ただし、干渉情報ログ・パケットログ・統計情報ログの 3 つのログは、情報量が膨大な為、WEB コンソール・CLI コンソールでのログ読出しができません。

※ 干渉情報ログ・パケットログ・統計情報ログはバイナリデータであり、バイナリ転送モードで読み出す必要があります。
※ TFTP は UDP 接続で信頼性に欠けるため、大容量ファイルを転送する場合は FTP をご使用ください。

6.3.2　記録・表示

本装置のログを記録・表示するための手順をここで紹介します。

操作手順

◆ログ機能の有効化

ログ機能を有効にするために、監視制御設定を行います。

手順1　〔保守〕→〔監視制御設定〕を選択します。

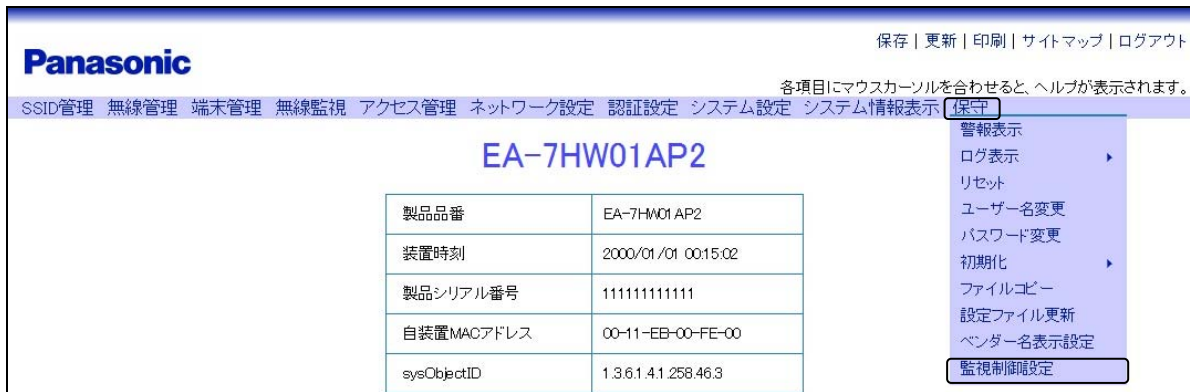



図6.3-1　メニュー（監視制御設定）

手順2　監視制御の〔ON〕を選択し、〔設定〕ボタンをクリックします。

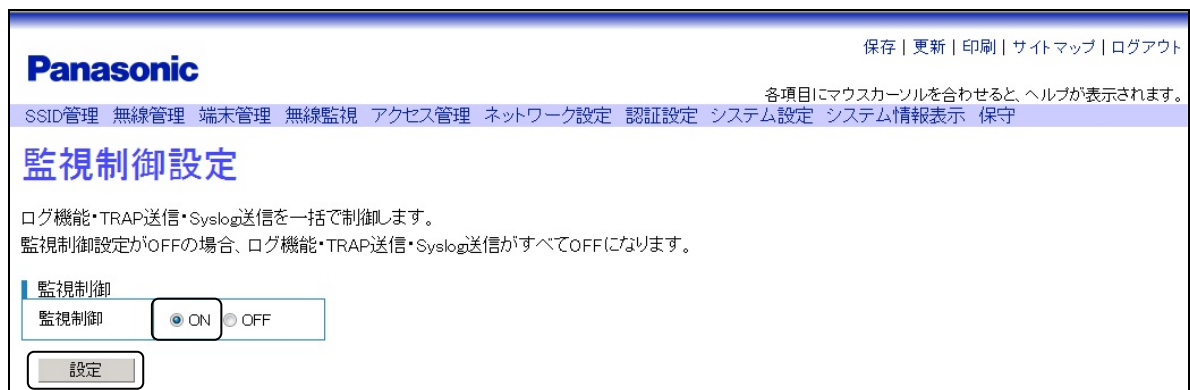



図6.3-2　監視制御設定

※　このオプションは、ログ機能だけでなく、ログ機能・TRAP 送信・Syslog 送信などすべての監視制御機能の ON/OFF を一括で切り替えます。

手順3　画面右上の〔保存〕ボタンをクリックし、設定した内容を本装置に保存します。

◆ログのファイル名設定

各種ログファイルのファイル名を設定します。

手順4　〔システム設定〕　→　〔運用設定〕　→　〔ファイル名設定〕を選択します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

運用設定　監視インターフェース設定　監視設定

装置設定　トラフィック監視設定　ログ設定　ファイル名設定

EA-7HW01AP

製品品番	EA-7HW01 AP2

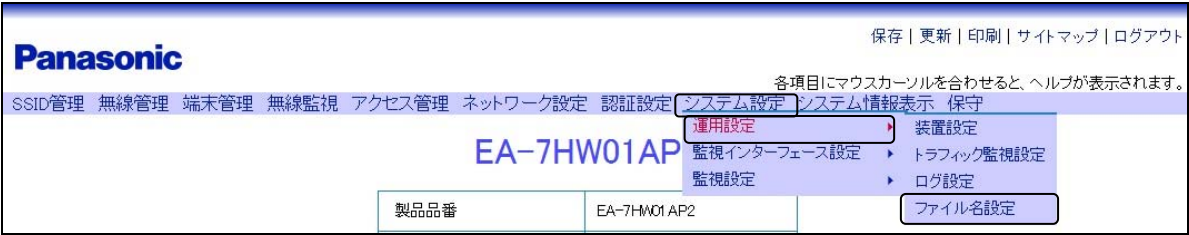



図6.3-3　メニュー（ファイル名設定）

手順5　各種ログのファイル名を入力します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

ファイル名設定

項目	ファイル名
自装置ファームウェア(1面)	apfirmware
自装置ファームウェア(2面)	firmware2
設定ファイル	setting
イベントログファイル	eventlog
TRAPログファイル	traplog
AP管理ログファイル	aplog
端末管理ログファイル	stationlog
監視アクセスログファイル	accesslog
コマンドログファイル	commandlog
シーケンスログファイル	sequentiallog
干渉情報ログファイル	interferencelog
パケットログファイル	packetlog
統計情報ログファイル	statisticslog

図6.3-4　ファイル名設定

手順6　画面最下部の〔設定〕ボタンをクリックし、設定を反映させます。

◆ログの記録方法の設定

ログの取得方法など、ログの記録に関する詳細設定を行います。

手順7　〔システム設定〕　→　〔運用設定〕　→　〔ログ設定〕を選択します。

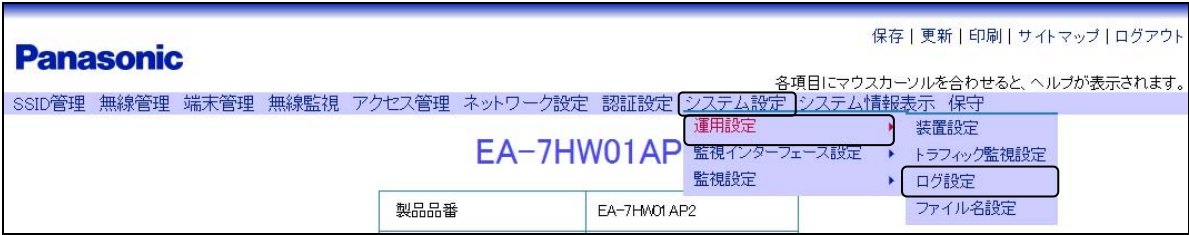



図6.3-5　メニュー（ログ設定）

※　手順８ ～ 手順 10 は〔ログ設定〕画面（図 6.3-6）より各種設定を行います。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

ログ設定

ログに関する設定を行います。

- 監視制御状態
- ログ全体設定
- 各ログの設定①
- 各ログの設定②
- 表示モード設定

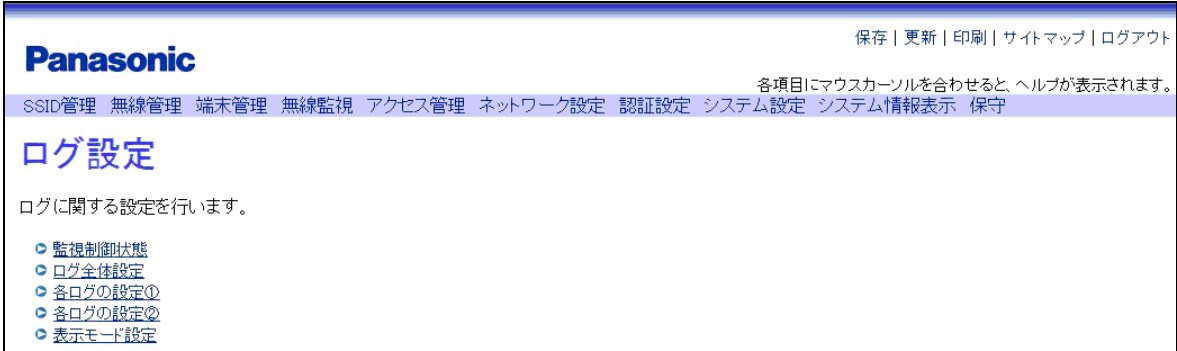



図6.3-6　ログ設定

手順8　〔ログ設定〕画面（図 6.3-6）の〔ログ全体設定〕をクリックし、〔有効〕を選択します。

図6.3-7　ログ全体設定

手順9　〔ログ設定〕画面（図 6.3-6）の〔各ログの設定①〕をクリックし、各ログの取得モードを選択します。

例として、すべて〔wrap〕を選択します。

図6.3-8　各ログの設定①

表6.3-2　ログ取得モード

モード名称	説明
wrap	ログが最大件数に達した場合に、最古のレコードから上書き保存します。
halt	ログが最大件数に達した場合は、それ以上ログ取得を行いません。 ログ消去でログ取得を再開します。
off	ログ取得は行いません。

手順10　〔ログ設定〕画面（図 6.3-6）の〔各ログの設定②〕をクリックし、ログの取得設定を行います。
例として、パケットログ・統計情報ログの取得を〔有効〕にします。

図6.3-9　各ログの設定②

手順11　画面最下部の〔設定〕ボタンをクリックし、設定を反映させた後、画面右上の〔保存〕ボタンをクリックし、設定した内容を本装置に保存します。

以上の操作／設定により、ログを記録することができます。

◆ログデータの表示
「◆ログ機能の有効化」、「◆ログの記録方法の設定」を行って記録したログは、Web コンソール上で簡単に表示、確認できます。
ここでは、例としてコマンドログを表示する方法を紹介します。

手順12 〔保守〕 → 〔ログ表示〕 → 〔コマンドログ〕を選択します。

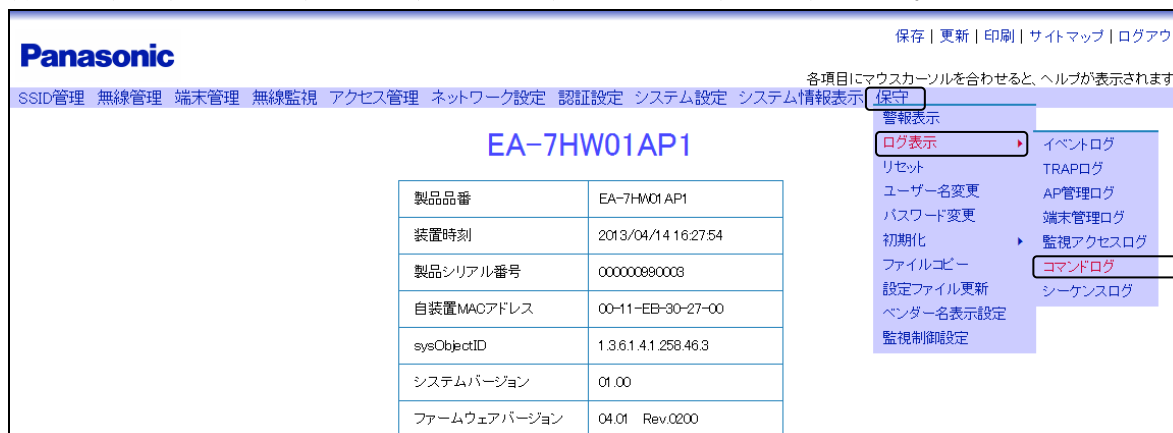



図6.3-10 メニュー（ログ表示）

以下の画面は、コマンドログの表示例です。

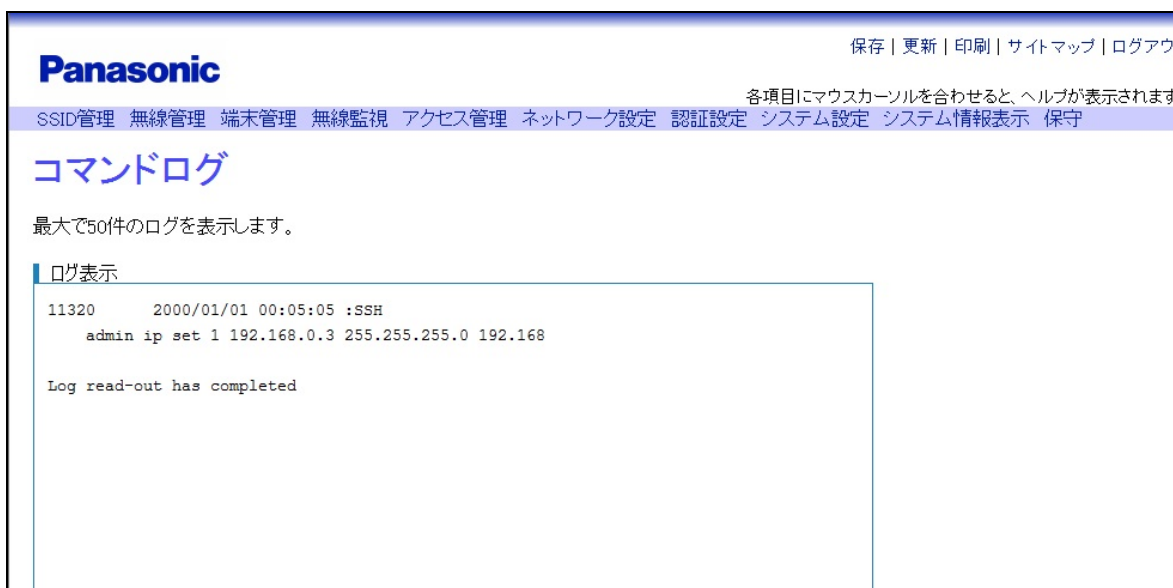



図6.3-11 コマンドログ

◆その他ログの読出し
本装置では、WEB 画面でのログ表示以外に、下記表（表 6.3-3 ログ読出し方法）に記載している方法でのログ取得も行えます。

表6.3-3 ログ読出し方法

	説明
コマンドライン	通信ソフトを使用して、コマンド入力によりレコード単位に読み出しを行います。（別紙「コマンドリファレンス」参照）
TFTP	TFTP プロトコルにより一括読み出しを行います。（「6.3.3 FTP/TFTP によるリモート採取」参照）
syslog	syslog プロトコルにより syslog サーバーへリアルタイムにログを転送します。（イベントログ、AP 管理ログ、端末管理ログのみ）

6.3.3 TFTPによるリモート採取

操作手順

◆TFTP サーバーへのログファイルコピー

ログの記録は、前項ですでに済んでいるという前提で解説をします。

手順1　〔システム設定〕　→　〔監視設定〕　→　〔TFTP 設定〕をクリックします。

図6.3-12　メニュー（TFTP 設定）

手順2　TFTP サーバーとの通信に関する設定を入力します。

例として、下記内容での設定を示します。

・ IP インターフェース番号に〔1〕を選択
・ サーバー指定方法に〔IP アドレス〕を選択
・ IP アドレス／ドメイン名に「192.168.0.99」（TFTP サーバーのアドレス）を入力

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守

TFTP設定

TFTPに関する設定を行います。
TFTP機能を動作させる場合は、アクセス許可設定を「許可」にしてください。

TFTP設定

アクセス許可設定	◉許可 ○禁止
IPインターフェース番号 一覧参照	1
サーバー指定方法	◉IPアドレス ○ドメイン名
IPアドレス／ドメイン名 ※1	192.168.0.99

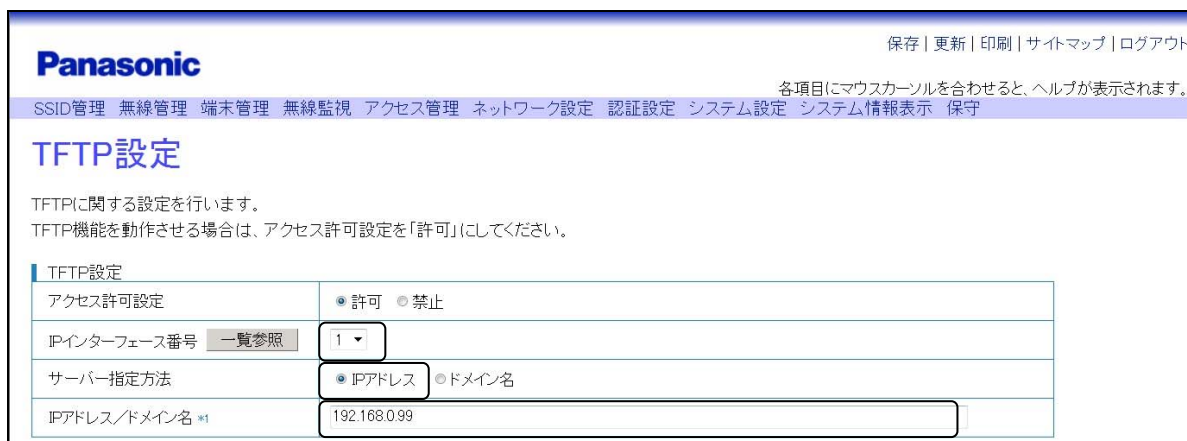



図6.3-13　TFTP 設定

手順3　TFTP 設定下部の〔設定〕ボタンをクリックし、設定を反映させます。

手順4　〔システム設定〕　→　〔運用設定〕　→　〔ファイル名設定〕を選択します。

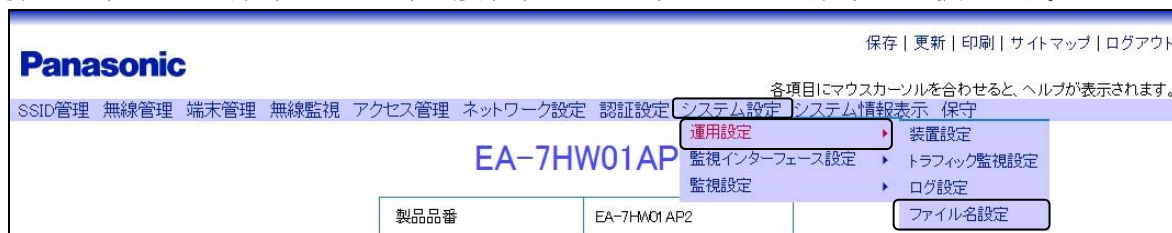



図6.3-14　メニュー（ファイル名設定）

手順5　取得するログのファイル名を設定します。

例として、コマンドログを「command01」と設定します。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守

ファイル名設定

自装置の各種ファイルを制御する際に使用するファイル名を設定します。
ファイル名は、半角英数字またはアンダーライン(_)・ハイフン(-)・ピリオド(.) 0〜31文字以内で入力してください。

ファイル名設定

自装置ファームウェア(1面)	firmware1
自装置ファームウェア(2面)	firmware2
設定ファイル	config
イベントログファイル	eventlog
TRAPログファイル	traplog
AP管理ログファイル	aplog
端末管理ログファイル	stationlog
監視アクセスログファイル	accesslog
コマンドログファイル	command01

図6.3-15　ファイル名設定

手順6　画面最下部の〔設定〕ボタンをクリックし、設定を反映させた後、画面右上の〔保存〕ボタンをクリックし、設定した内容を本装置に保存します。

手順7　〔保守〕　→　〔ファイルコピー〕を選択する。

図6.3-16　メニュー（ファイルコピー）

手順8　ファイルコピー方法とコピーするファイルを指定します。

例として、下記内容での設定を示します。

・ デバイス選択（コピー元→コピー先）で〔自装置→TFTP サーバー〕を選択

・ コピーファイルに「command01」を入力

選択、および入力後、画面左下の〔コピー〕ボタンをクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト

Panasonic

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

SSID管理　無線管理　端末管理　無線監視　アクセス管理　ネットワーク設定　認証設定　システム設定　システム情報表示　保守

ファイルコピー

指定ファイルを選択したデバイス間でコピーします。
コピーできるファイルの種別は、選択したデバイスによって異なります。

ファイルコピー

デバイス選択 *1	自装置 → TFTPサーバー
コピーファイル *1 *2　一覧参照	command01　(1～31文字)

図6.3-17　ファイルコピー

以上の操作により、TFTP サーバーに「コマンドログ」がコピー保存されます。

◆FTP によるログファイルコピー

FTP コマンドを使用してログファイルをコピーする場合、「6.1.1　設定データのバックアップ」を参照し FTP でログインします。ログイン後、「コマンド：“get command01”」を実行します。

6.3.4　ログの初期化

ログの初期化には、すべてのログを一括で初期化する方法と、各ログを個別に初期化する方法があります。
それぞれの手順を以下に示します。

操作手順

◆全ログクリアー

手順1　〔保守〕　→　〔初期化〕　→　〔ログ初期化〕を選択します。

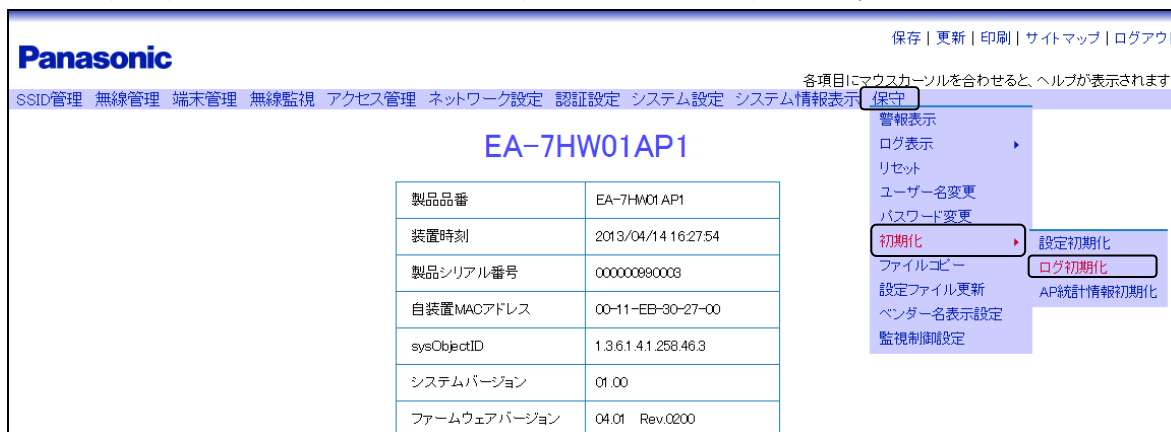



図6.3-18　メニュー（ログ初期化）

手順2　全ログクリアーの〔全ログ〕のチェックボックスをクリックします。

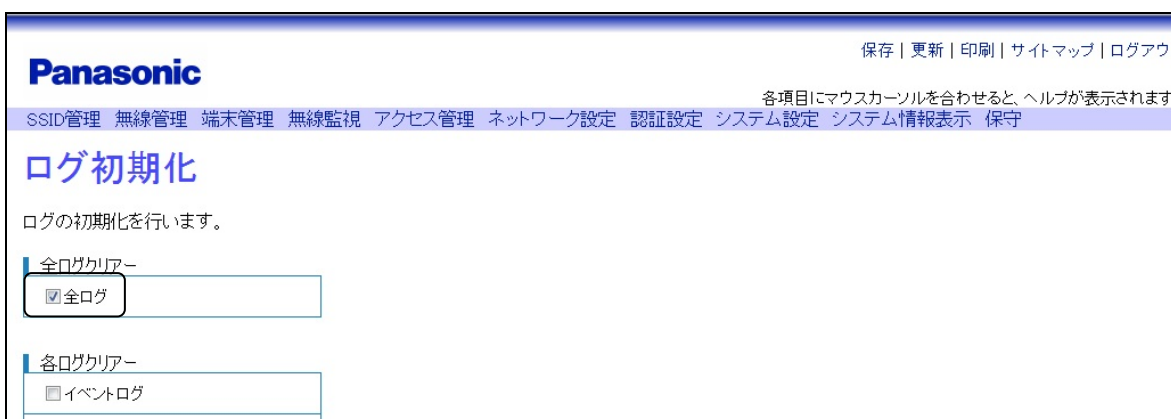



図6.3-19　ログ初期化（全ログクリアー）

手順3　画面最下部の〔実行〕ボタンをクリックします。

以上の操作により、すべてのログが削除されます。

◆各ログクリアー

例として、コマンドログの削除方法を紹介します。

手順1　〔保守〕　→　〔初期化〕　→　〔ログ初期化〕を選択します。

手順2　各ログクリアーの〔コマンドログ〕のチェックボックスをクリックします。

図6.3-20　ログ初期化（コマンドログクリアー）

手順3　画面最下部の〔実行〕ボタンをクリックします。

以上の操作により、コマンドログが削除されます。

6.3.5　干渉情報ログ・パケットログ・統計情報ログの読出し

本装置では、干渉情報ログ・パケットログ・統計情報ログの記録／読出しを行うことができます。
読出し時は、ログ記録時の時刻を算出するために、ログデータの前にログ読出し時の現在時刻とログ読出し時の情報蓄積時間（sysUpTime）も読み出します。
各ログの記録方法は、「6.3.2　記録と表示」の　◆ログ機能の有効化、◆ログのファイル名設定、◆ログの記録方法の設定を参照してください。
ログが上限まで取得できていない場合は、蓄積分のみ取得可能です。

操作手順

手順1　〔保守〕　→　〔ファイルコピー〕を選択する。

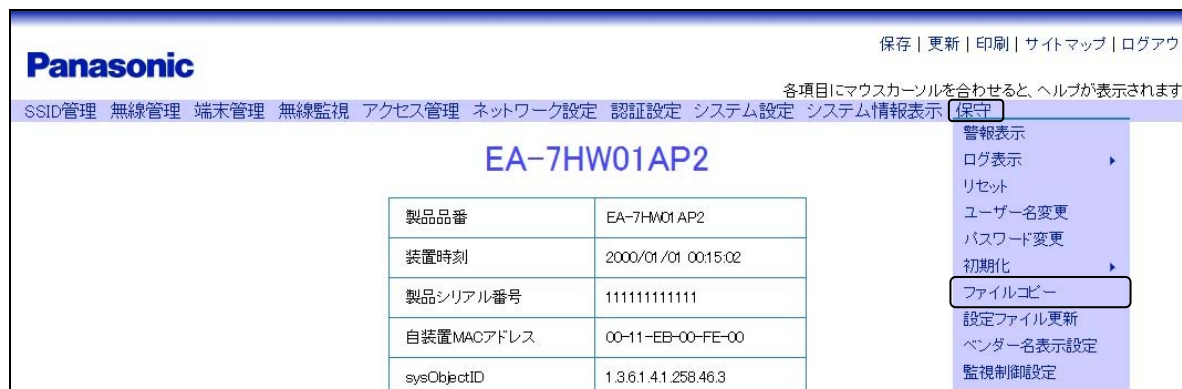



図6.3-21　　メニュー（ファイルコピー）

手順2　パケットログを TFTP サーバーにコピーします。

以下の操作を行います。

- デバイス選択の〔自装置 → TFTP サーバー〕を選択
- コピーファイル名に ◆ログのファイル名設定で設定したファイル名を入力
  ここでは、「packetlog」を入力します。選択、および入力後、〔コピー〕をクリックします。

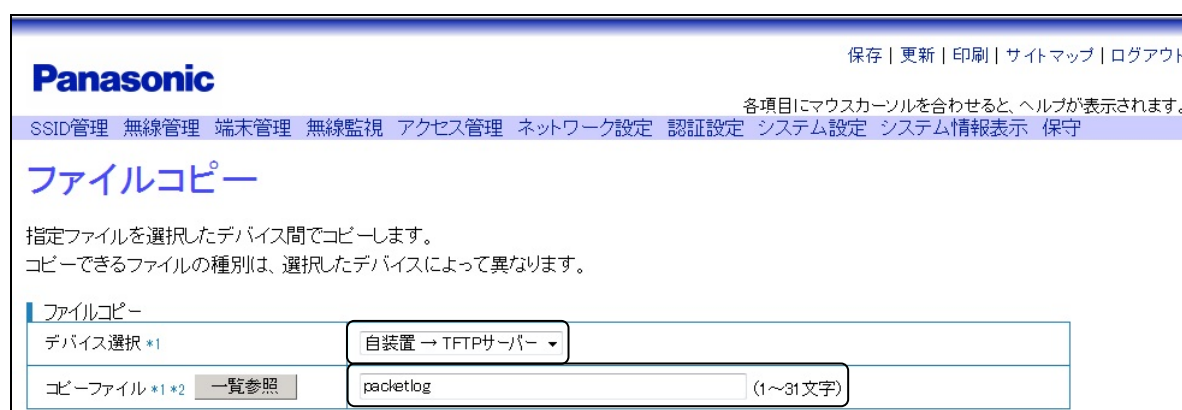



図6.3-22　　ファイルコピー（パケットログ）

以上の操作により、TFTP サーバーにパケットログがコピーされます。

6.4　遠隔無線通信状態の確認

本装置では、無線フレームが実際に送信されているかどうかを確認する無線送信検出機能を持ちます。
本機能は、無線フレームの送信状態を確認したい無線インターフェースを指定し、その無線インターフェースで送信した無線フレームを反対側の無線インターフェースで受信することにより、無線フレームの送信ができていることを確認する機能です。そのため、両無線インターフェースが有効の場合のみ検出処理を行います。どちらかの無線インターフェースが無効な場合は検出失敗となります。
なお、本機能では、ビーコンフレームを検出対象として使用します。

受信側の無線インターフェースで送信側のビーコンを受信した場合は、検出処理を終了します。
検出できない場合は、3 秒間検出処理を継続し、検出時間が満了した場合は、検出失敗（タイムアウト）として、検出処理を終了します。
※両無線インターフェース有効時に検出側の無線インターフェースのビーコン送信が無効に設定されている場合は、検出失敗（タイムアウト）となります。

重要	■ 通信状態検出処理中は、受信側の無線インターフェースを検出用に使用するため、受信側のビーコンフレームの送信は行いません。そのため、受信側の無線インターフェースでは、接続中の端末から切断される可能性があります。本装置からの端末切断処理は行いません。

操作手順

手順1　〔無線管理〕　→　〔無線制御〕を選択します。

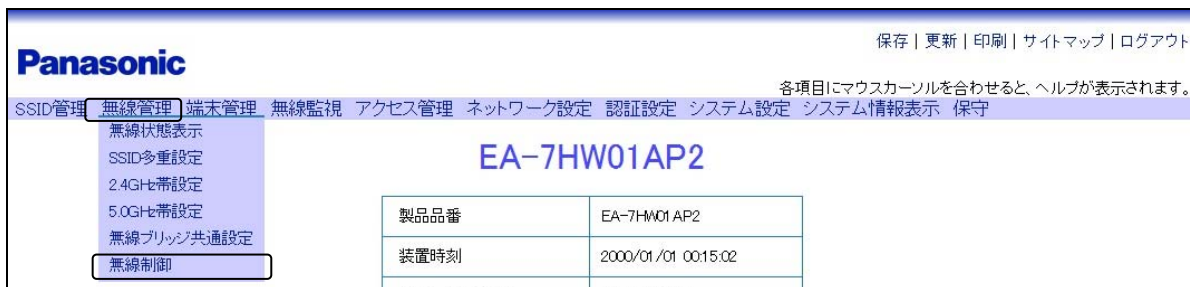



図6.4-1　メニュー（無線制御）

手順2　〔無線送信検出〕をクリックします。

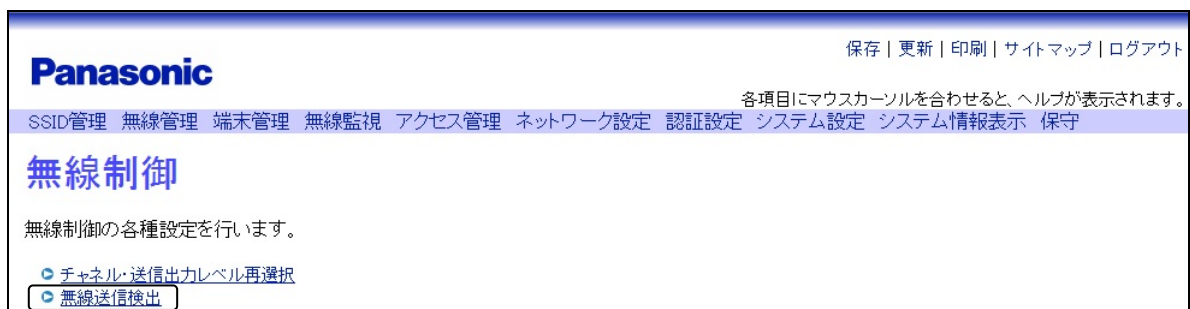
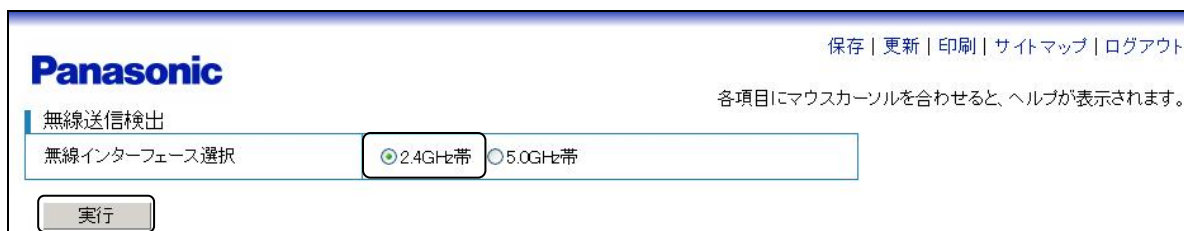



図6.4-2　無線制御

手順3　無線送信検出を実行します。

ここで選択した無線インターフェースを検出対象とします。
例として、〔2.4GHz 帯〕を選択します。

図6.4-3　無線制御送信検出

手順 3 実行後、下図の検出結果のダイアログボックスが表示されます。

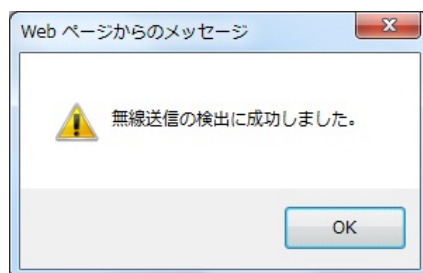



図6.4-4　検出成功時

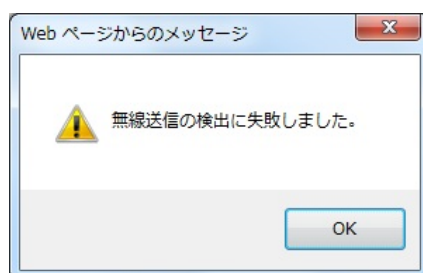



図6.4-5　検出失敗時

6.5　時刻設定

Web コンソールから本装置の時刻を設定できます。時刻設定方法として、手動による時刻設定と NTP クライアント機能を使用した時刻設定の 2 種類をサポートしています。

<NTP について>
ネットワーク機器の内部時計を、ネットワークを介して正しく調整する プロトコルです。階層構造を持ち、最上位の サーバーが GPSなどを利用して正しい時刻を得て、下位のホストはそれを参照することで時刻を合わせます。

はじめに、手動による時刻設定の方法を示します。

操作手順

手順1　〔システム設定〕　→　〔運用設定〕　→　〔装置設定〕を選択します。

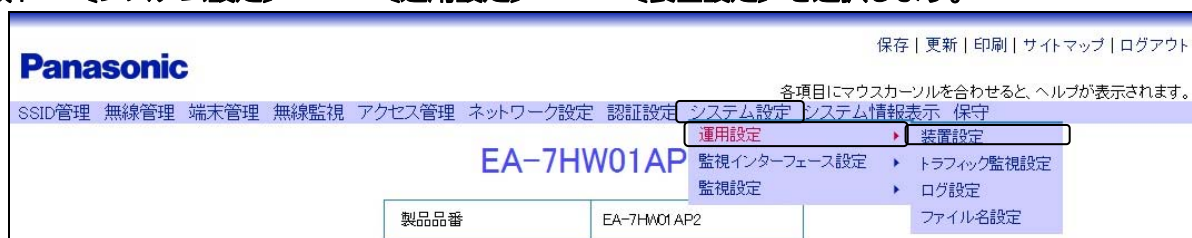



図6.5-1　メニュー（装置設定）

手順2　〔装置時刻〕をクリックします。

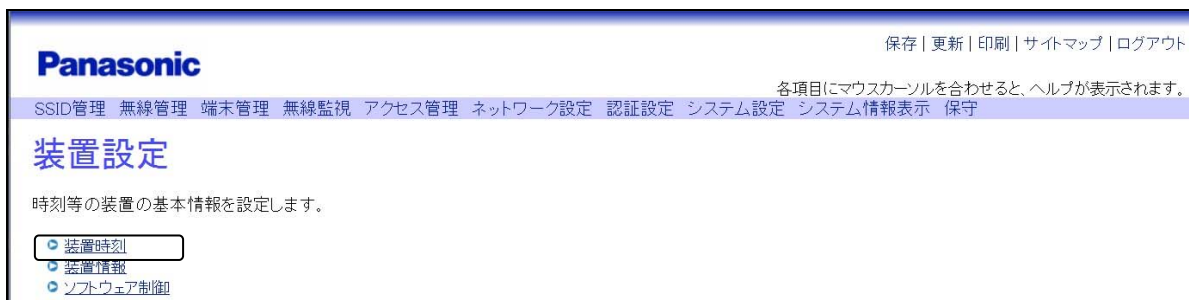



図6.5-2　装置設定

手順3　装置時刻を入力します。
例として、「2012/12/15 09:30:00」を入力します。
入力後、画面下部の〔設定〕ボタンをクリックして本装置に反映させます。

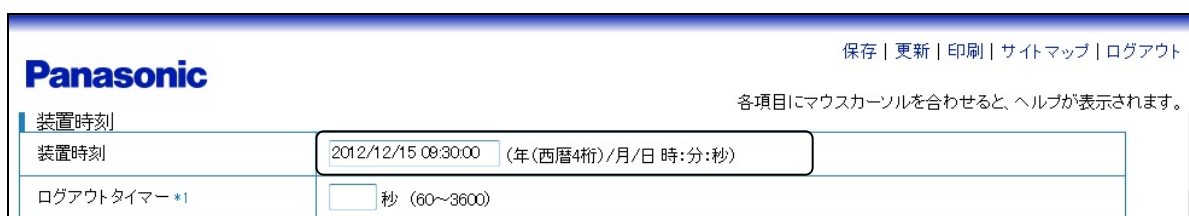



図6.5-3　装置時刻

以上の操作により、手動による時刻設定が行えます。

重要	■ 装置のリセットやコマンド入力による設定初期化および WEB での設定初期化（6.6　装置の初期化参照）を実行しても時刻の設定は初期化されることはありませんが、電源 OFF/ON で時刻が最大で 1 日巻き戻ります。また INIT スイッチによる初期化（6.6　装置の初期化参照）では時刻が「2000/1/1 00:00:00」に初期化されます。NTP クライアント機能を使用した時刻設定を行った場合は自動で時刻が補正されますが、設定を行っていない場合、電源 OFF/ON および INIT スイッチによる初期化の際には、必ず時刻設定を行ってください。 ■ ログ機能や IPsec 機能は装置時刻を参照していますので、これらの機能を正常に動作させるために、必ず時刻の設定を行ってください。

続いて、NTP クライアント機能を使用した時刻設定を以下に示します。

操作手順

手順1　〔システム設定〕　→　〔監視設定〕　→　〔NTP 設定〕を選択します。

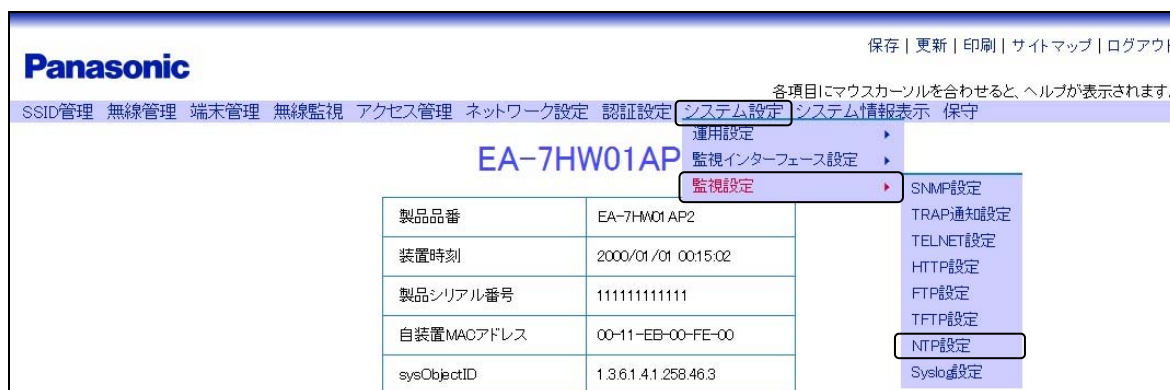



図6.5-4　メニュー（監視設定）

手順2　〔NTP 設定〕をクリックします。

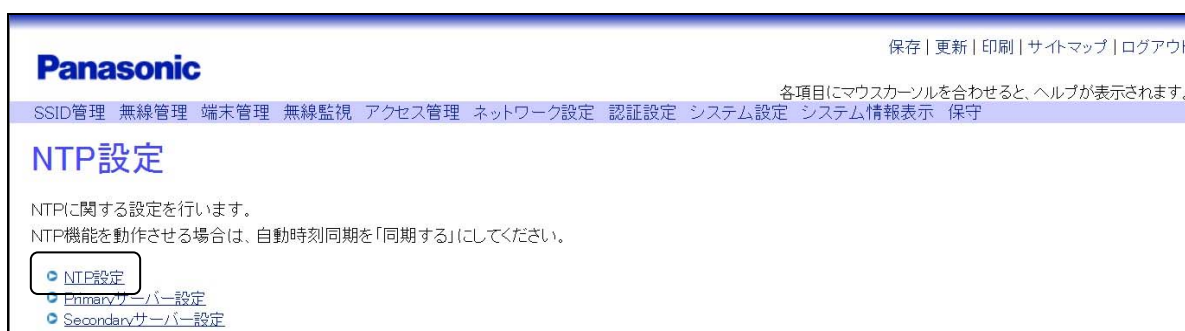



図6.5-5　NTP 設定

手順3　〔NTP 設定〕画面にて、〔同期する〕を選択します。

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

NTP設定

自動時刻同期	◉同期する ○同期しない
時刻同期間隔 *1	60 分（1～1440）

図6.5-6　NTP 設定

手順4　〔Primary サーバー設定〕画面にて、NTP サーバー（Primary）を設定します。

例として、下記内容での設定を示します。

- IP インターフェース番号 :〔1〕を選択
- サーバー指定方法 :〔IP アドレス〕を選択
- IP アドレス／ドメイン名 :「192.168.0.76」を入力

Panasonic

保存 | 更新 | 印刷 | サイトマップ | ログアウト

各項目にマウスカーソルを合わせると、ヘルプが表示されます。

Primaryサーバー設定

IPインターフェース番号 一覧参照	1
サーバー指定方法	◉IPアドレス ○ドメイン名
IPアドレス／ドメイン名 *2	192.168.0.76

図6.5-7　Primary サーバー設定

手順5　〔Secondary サーバー設定〕画面にて、NTP サーバー（Secondary）を設定します。

例として、下記内容での設定を示します。

- IP インターフェース番号 :〔1〕を選択
- サーバー指定方法 :〔IP アドレス〕を選択
- IP アドレス／ドメイン名 :「192.168.0.79」を入力

入力後、画面下部の〔設定〕ボタンをクリックして本装置に反映させます。

図6.5-8　Secondary サーバー設定

以上の操作により、NTP クライアント機能を使用した時刻設定が行われます。

手順 3、4 の「サーバー指定方法」で〔ドメイン名〕を選択する場合は、あらかじめ DNS サーバーの設定が必要です。

6.6　装置の初期化

本装置が持つ各種情報の初期化を行います。初期化方法は 3 種類あり、初期化される情報が異なります。

表6.6-1　初期化の種別一覧

初期化方法	初期化される情報
INIT スイッチ	すべての装置情報（設定データ、ログデータ、時刻情報、IKE 証明書データ）を工場出荷時の値にします。
コマンド入力	初期化を行いたい設定データ、またはログデータを指定することで、指定した情報のみを工場出荷時の値にします。
WEB	管理用インターフェースに関する設定以外、すべて初期化します。

※ 初期化を行った場合、元の状態に戻せなくなりますので、バックアップデータを取得する等、十分注意して行ってください。

操作手順

◆INIT スイッチでの設定初期化

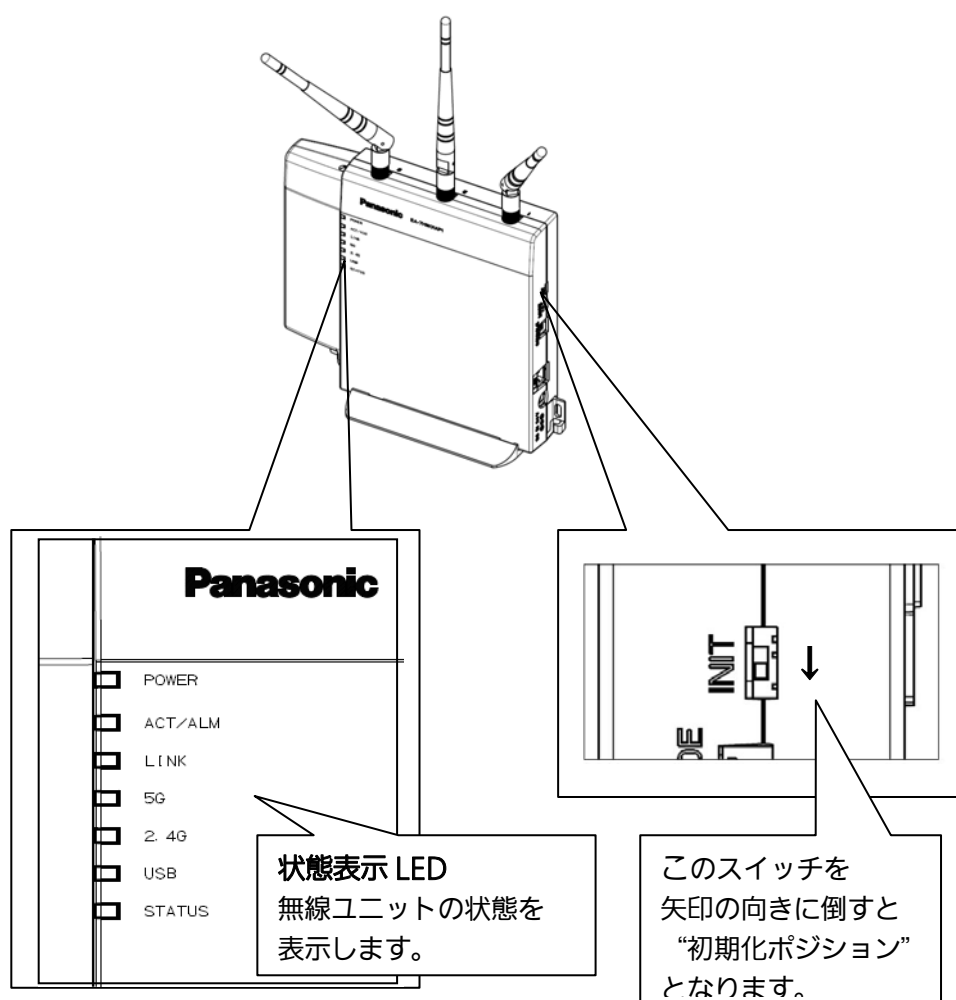



図6.6-1　屋内用無線 LAN アクセスポイント配置説明

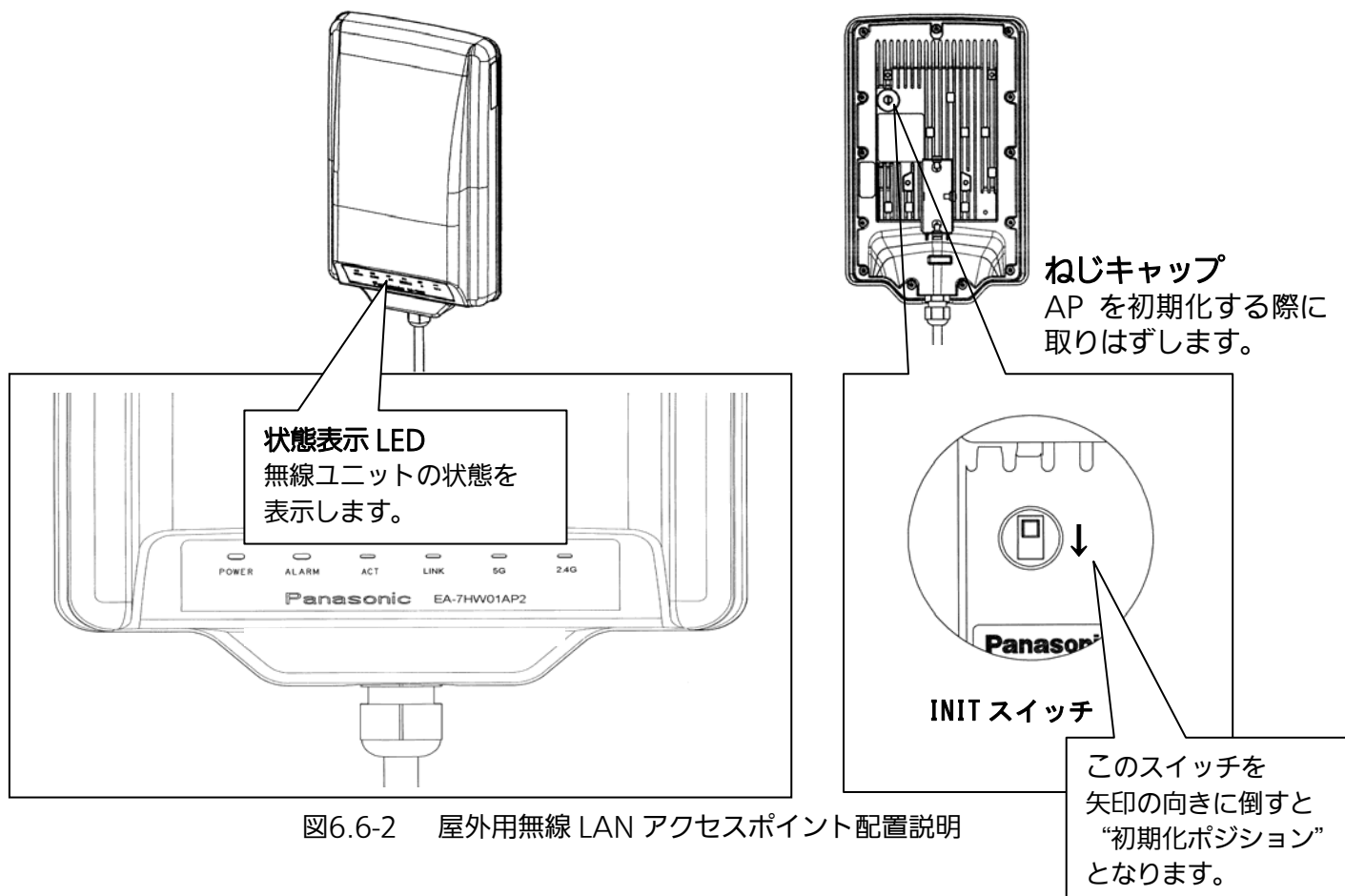



図6.6-2　屋外用無線 LAN アクセスポイント配置説明

手順1　本装置の電源を切ります。

手順2　屋内用無線 LAN アクセスポイントの場合、INIT スイッチを初期化ポジション（図 6.6-1 参照）にスライドさせせます。屋外用無線 LAN アクセスポイントの場合は裏側のねじキャップをとりはずし、INIT スイッチを初期化ポジション（図 6.6-2 参照）にスライドさせせます。

手順3　本装置 の電源を入れ、前面の LED が点灯・点滅（屋内用無線 LAN アクセスポイントは ACT/ALM LED : 点滅、屋外用無線 LAN アクセスポイントは ALM LED : 点滅）となるまで待ちます。

手順4　10 秒以上経過したら、再度本装置 の電源を切ります。（10 秒以上経過しても LED の点灯・点滅状態は変わりません。）

手順5　INIT スイッチを通常運用ポジションに戻します。

手順6　屋外機の場合はとりはずしたねじキャップを取りつけます。

手順7　本装置の電源を入れます。

以上で、INIT スイッチの操作による初期化が完了です。

◆コマンド入力による設定初期化

コンソールの接続が完了している前提で説明します。（コンソール接続方法は、2.4 CLI コンソールでのログイン・ログアウトを参照）

手順1　設定の初期化コマンドを入力して、実行します。

```
# initial config all
  ↑　初期化コマンドを入力します。
```

手順2　確認メッセージ表示後、"y"を入力して、実行します。

```
# initial config all
"initialize"　and　"reset"　y or n >>
  ↑　"y"　は「リセットし、初期化させる」、"n"　は「リセットせず、初期化させない」
    となります。
```

上記「手順 2」実施後、本装置が再起動し、設定データの初期化が完了します。

◆WEB での設定初期化

手順1　〔保守〕　→　〔初期化〕　→　〔設定初期化〕を選択します。

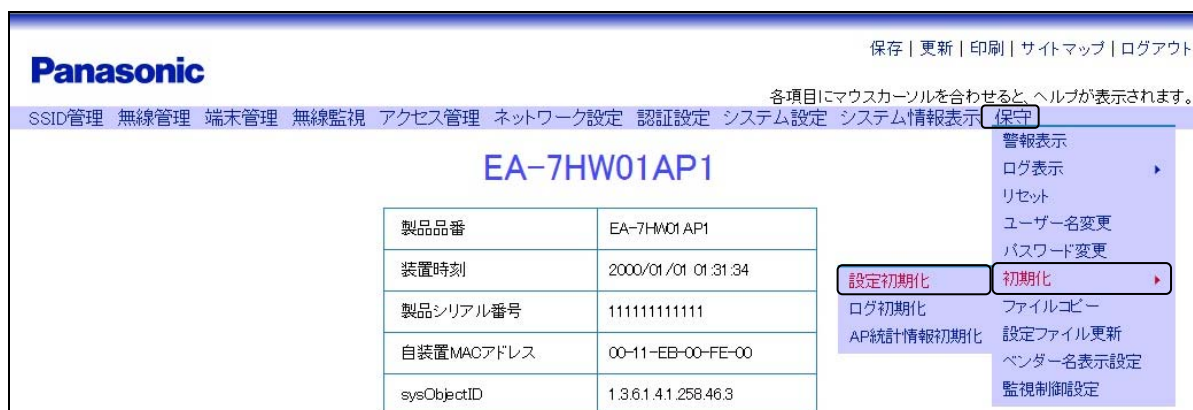



図6.6-3　メニュー（設定初期化）

手順2　〔クリアー〕ボタンをクリックします。

保存 | 更新 | 印刷 | サイトマップ | ログアウト
Panasonic
各項目にマウスカーソルを合わせると、ヘルプが表示されます。
SSID管理 無線管理 端末管理 無線監視 アクセス管理 ネットワーク設定 認証設定 システム設定 システム情報表示 保守
設定初期化
設定の初期化を行います。
全設定クリアー(管理用インターフェースに関する設定以外)
クリアー

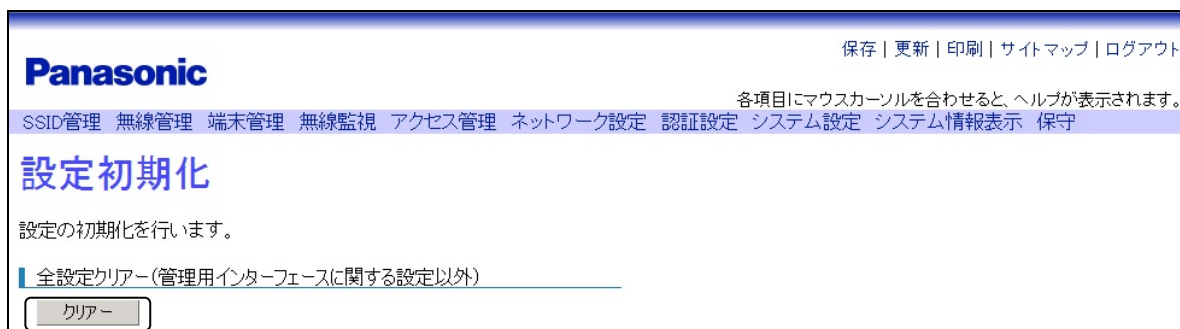



図6.6-4　設定初期化

手順3　確認メッセージの〔OK〕ボタンをクリックします。

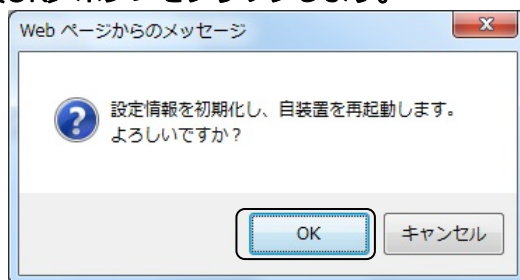



図6.6-5　初期化確認メッセージ

上記「手順 3」実施後、本装置が再起動し、設定データの初期化が完了します。

保証とアフターサービス(よくお読みください)

使いかた・お手入れ・修理などは

■まず、お買い求め先へご連絡ください。

▼お買い上げの際に記入されると便利です

販売店名

電話　（　　）　－

お買い上げ日　年　月　日

修理を依頼されるときは

取扱説明書(設計・工事編)「障害発生時の対処方法」（73 ページ）でご確認のあと、
直らないときは、AC 電源装置（PoE インジェクタ、AC アダプタ）の電源プラグを抜いて、
お買い上げ日と下記の内容をご連絡ください。

● 製品名	屋内用/屋外用無線 LAN アクセスポイント
● 品番	EA-7HW01AP1 / EA-7HW01AP2
● 故障の状況	できるだけ具体的に

●保証期間中に本製品が通常の使用状態で不良になった場合、修理は無償で実施します。

保証期間：お買い上げ日から本体 1 年間

●保証期間終了後は、診断をして修理できる場合はご要望により修理させていただきます。

※修理料金は次の内容で構成されています。

技術料	診断・修理・調整・点検などの費用
部品代	部品および補助材料代
出張料	技術者を派遣する費用

※補修用性能部品の保有期間 7 年

当社は、本製品の補修用性能部品（製品の機能を維持するための部品）を、
製造打ち切り後 7 年保有しています。

■その他ご不明な点は下記へご連絡ください。

パナソニック　システムお客様ご相談センター

電話　フリーダイヤル

携帯電話・PHS からもご利用いただけます。

受付時間：9 時 ～ 17 時 30 分（土・日・祝祭日は受付のみ）

ホームページからのお問い合わせは

https://sec.panasonic.biz/solution/info/

ご使用の回線（IP 電話やひかり電話など）によっては、回線の混雑時に数分で切れる場合があります。

【ご相談窓口におけるお客様の個人情報のお取り扱いについて】

パナソニック株式会社およびグループ関係会社は、お客様の個人情報をご相談対応や修理対応などに利用させていただき、ご相談内容は録音させていただきます。また、折り返し電話をさせていただくときのために発信番号を通知いただいております。なお、個人情報を適切に管理し、修理業務等を委託する場合や正当な理由がある場合を除き、第三者に開示・提供いたしません。
個人情報に関するお問い合わせは、ご相談いただきました窓口にご連絡ください。

この商品は外国為替及び外国貿易法に定める規制貨物に該当しますので、輸出される場合には、同法の規制を確認の上、輸出許可取得等の手続きをお取りください。
（平成 25 年 5 月現在）

パナソニック システムネットワークス株式会社

〒２２４-８５３９　神奈川県横浜市都筑区佐江戸町６００番地

N0113-1053